

Advanced Small Modular Reactor (SMR) Probabilistic Risk Assessment (PRA) Technical Exchange Meeting

Curtis Smith

September 2013



The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-13-30170

Advanced Small Modular Reactor (SMR) Probabilistic Risk Assessment (PRA) Technical Exchange Meeting

Curtis Smith

September 2013

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

<http://www.inl.gov>

**Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**

1.1 Overview

A key area of the Advanced Small Modular Reactor (SMR) Probabilistic Risk Assessment (PRA) strategy is the development of methodologies and tools that will be used to predict the safety, security, safeguards, performance, and deployment viability of SMR systems starting in the design process through the operation phase. The goal of the SMR PRA activity will be to develop quantitative methods and tools and the associated analysis framework for assessing a variety of risks. These risks will be focused on SMR designs and operational strategies as they relate to the technical basis behind safety and security characterization.

Development and implementation of SMR-focused safety assessment methods may require new analytic methods or adaptation of traditional methods to the advanced design and operational features of SMRs. We will need to move beyond the current limitations such as static, logic-based models in order to provide more integrated, scenario-based models based upon predictive modeling which are tied to causal factors. The development of SMR-specific safety models for margin determination will provide a safety case that describes potential accidents, design options (including postulated controls), and supports licensing activities by providing a technical basis for the safety envelope.

During FY13, the INL developed an advanced SMR PRA framework which has been described in the report *Small Modular Reactor (SMR) Probabilistic Risk Assessment (PRA) Detailed Technical Framework Specification*, INL/EXT-13-28974 (April 2013). In this framework, the various areas are considered:

- Probabilistic models to provide information specific to advanced SMRs
- Representation of specific SMR design issues such as having co-located modules and passive safety features
- Use of modern open-source and readily available analysis methods
- Internal and external events resulting in impacts to safety
- All-hazards considerations
- Methods to support the identification of design vulnerabilities
- Mechanistic and probabilistic data needs to support modeling and tools

In order to describe this framework more fully and obtain feedback on the proposed approaches, the INL hosted a technical exchange meeting during August 2013. This report describes the outcomes of that meeting.

1.2 Technical Exchange Meeting Structure

The technical exchange meeting took place on August 21 and 22, 2013. The overall structure, topics, and presenters during the meeting are:

Introduction, Background and Agenda

The purpose of this meeting is to obtain stakeholder feedback on the Small Modular Reactor Probabilistic Risk Assessment Detailed Technical Framework Specification report published by the INL.

aSMR PRA, Safety, and Licensing Activities

Jim Kinsey – Idaho National Laboratory

Overview of the Advanced SMR PRA Framework

Curtis Smith – Idaho National Laboratory

Development of Surrogates for Core Damage Frequency and Large Early Release Frequency for Advanced Small Modular Reactors

George Flanagan – Oak Ridge National Laboratory

Identification of Initiating Events for aSMRs

Mike Muhlheim – Oak Ridge National Laboratory

NGNP Licensing Overview

Mark Holbrook – Idaho National Laboratory

Advanced PRA Methods for aSMRs

Diego Mandelli – Idaho National Laboratory

Cloud Technologies for use in Risk Assessment

Curtis Smith – Idaho National Laboratory

Risk-Informing Severe Accident Management Guidelines for aSMRs

Matthew Denman – Sandia National Laboratory

Review of Passive System Reliability Modeling Approaches for aSMRs

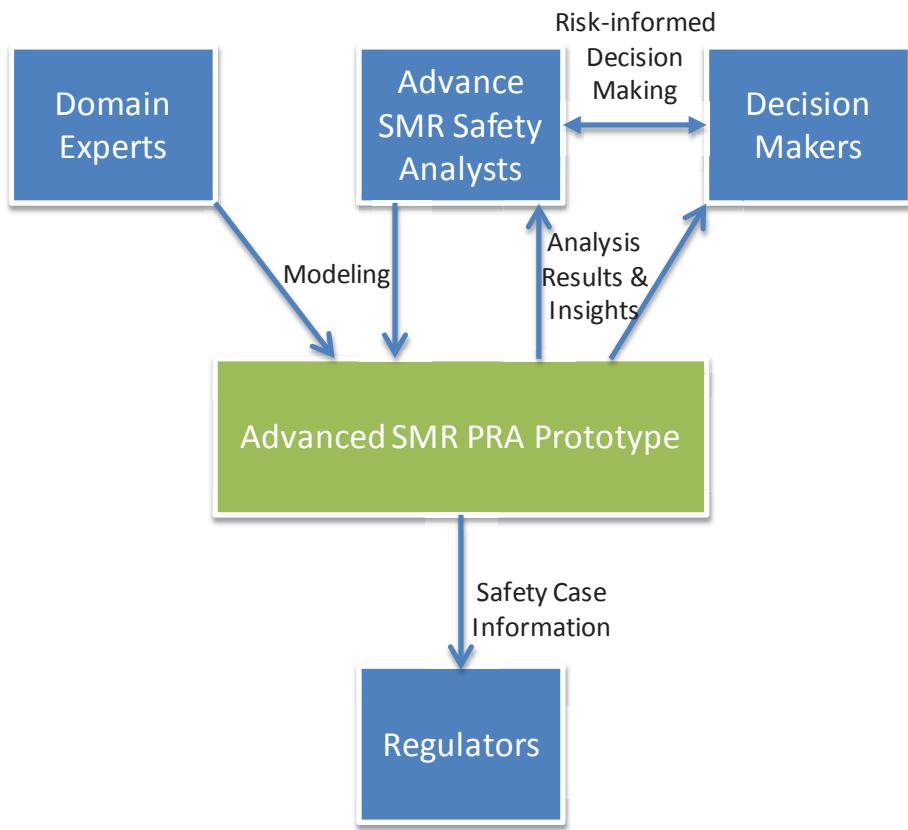
Dave Grabaskas – Argonne National Laboratory

3D Representation of Safety Hazards

Steve Prescott – Idaho National Laboratory

In addition to the presentations (slides of which are provided in Appendix A), discussion and question/answer sessions were facilitated. Included in the comments are:

- It would be helpful to find industry partners to play a role in the PRA prototype development.
- It was noted that the NRC will be (as part of its proposed NUREG-2150 activities) looking at “Design Enhancements.” These are called “Design Extension Conditions” by IAEA.
- Discussion was held related to whether untested passive features would work far in the future (e.g., 59 years later) in the context of aging and degradation mechanisms being present. An issue of inspectability seems to be more pressing for SMRs since they are (1) more integrated and (2) shipped (somewhat) prefabbled.
- It may be needed to make the initiating events list for advanced SMRs a “living document” to accommodate new issues, new ideas, and new modeling techniques as the project progresses. For example, if we move to simulating a variety of loss-of-coolant-accident (LOCA) break sizes, it may be that we simply have an initiating event called “LOCAs” rather than small LOCAs, medium LOCAs, large LOCAs, etc.
- It was noted for advanced reactors and passive designs that we should be able to find “cliff edge” effects at some (perhaps small in frequency) level in the risk analysis. Otherwise the regulator may not believe the analysis.
- The topic of using the Fukushima accident to benchmark an advanced flooding analysis may be a useful activity since a large quantity of information is available for that specific type of external event.
- Discussions were held concerning the need for a “generic” advanced SMR model that can be used by all of the analysis teams to provide a common-platform for our modeling and tool development.
- A question was asked about who is the primary target audience for the PRA framework? One response to this question was the following figure:



Attendees at the meeting were:

Amos, Willettia	DOE-Idaho
Denman, Matthew	Sandia National Laboratory
Flanagan, George	Oak Ridge National Laboratory
Grabaskas, David	Argonne National Laboratory
Holbrook, Mark	Idaho National Laboratory
Kinsey, Jim	Idaho National Laboratory
Munlheim, Mike	Oak Ridge National Laboratory
Prescott, Steve	Idaho National Laboratory
Sattison, Martin	Idaho National Laboratory
Smith, Curtis	Idaho National Laboratory
Sofu, Tanju	Argonne National Laboratory
Wheeler, Tim	Sandia National Laboratory
Youngblood, Bob	Idaho National Laboratory
Unwin, Stephen	Pacific Northwest National Laboratory

Appendix

A

Presentation Slides

The slides that were presented during the technical exchange meeting are listed in this Appendix.

Advanced SMR Safety and Licensing

Overview

Jim Kinsey
Regulatory Affairs Director
Idaho National Laboratory
U.S. Department of Energy

August 21, 2013

www.inl.gov



NRC 2012 Report to Congress – Safety Basis

The applicant's demonstration of the “safety case” supporting its license application requires comprehensive R&D to:

1. **Demonstrate safe performance** of the proposed design and applied technology,
2. **Provide the technical basis** for the application,
3. Demonstrate sufficient margins to safety-significant SSC design and safety limits,
4. **Search for and identify**, as well as assess and resolve, safety issues involving large uncertainties,
5. Develop, verify, and validate the proposed safety analysis evaluation methods,
6. **Provide the technical basis for requirements**, criteria, codes, or standards that are proposed for the licensing design basis,
7. **Quantify the failure thresholds** for safety-significant SSCs

Priority Advanced SMR Licensing Activities

- Licensing activities are focusing on areas that:
 - Could potentially have significant impact on the plant design and/or long duration research and development activities
 - Could potentially require Commission action
 - May represent a potentially significant license application content issue that could impact the application's acceptability or NRC review schedule

(It's noted that the list of topics that can be addressed at this point is constrained by the availability of plant design detail.)

Advanced SMR Licensing – Pathway Activities (FY13)

- Safety and Licensing
 - Licensing R&D
 - SMR site suitability and screening tools
 - Severe accident heat removal testing (NSTF at ANL)
 - Potential reduced requirements
- Safeguards
 - Safeguards and security
 - Proliferation resistance
- Probabilistic Risk Assessment (PRA)
 - PRA Methods – integrating operations, safeguards, security
 - Dynamic PRA – proof of concept

Advanced SMR Licensing Pathway Objectives

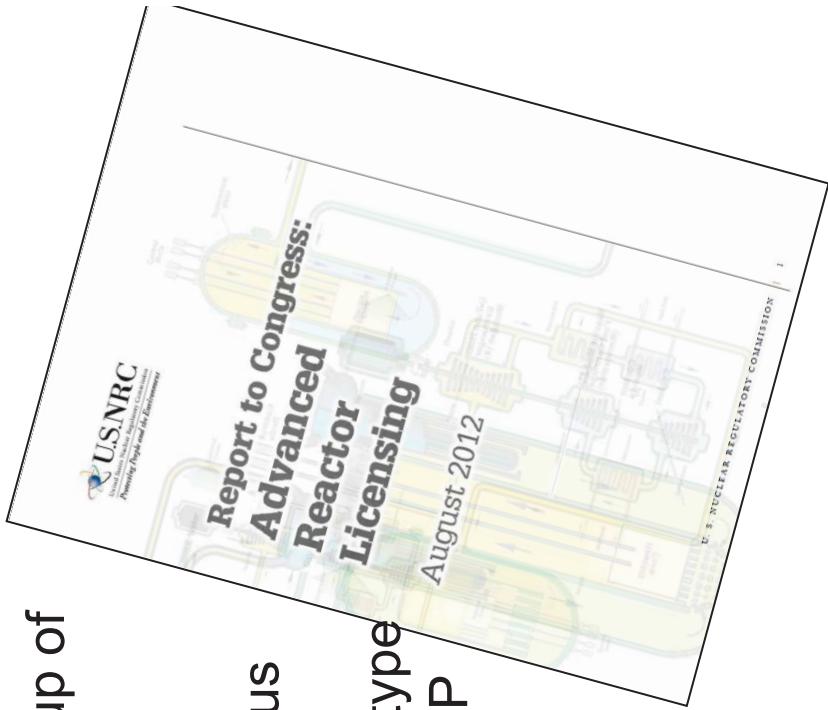
- A primary objective of the AdvSMR R&D Program is to facilitate the identification and conduct of R&D activities necessary to support licensing and deployment of advanced small modular reactor designs
- Collectively these R&D activities serve to reduce technology risks and facilitate licensing by the Nuclear Regulatory Commission (NRC)
- Current pathway focus is on addressing the most significant licensing issues early (FY13 work was a combination of “discovery” activities for future years and current implementation)

Plant Design Types

- The objective of the AdvSMR Program is to develop transformational technologies to enable next generation SMR designs to be deployed by 2030
- For efficiency, focus on a representative group of plant design types is required

- Safety and Licensing efforts will primarily focus on two technologies:
 - LMRs – with a focus on the SFR design type
 - HTGRs – leveraging work done via NGNP

(Other design types will be considered where possible and when adequate supporting information is available.)



Priority Safety and Licensing Items for FY14

- **Regulatory Framework Development**
 - General Design Criteria (GDCs) for advanced reactor technology
 - Joint initiative between DOE and NRC
- **Decay Heat Removal Testing**
 - Execute testing of the RCCS decay heat removal system
- **PRA Framework and Demonstration**
 - Develop an analysis and modeling prototype for advanced SMRs
 - Conduct a demonstration problem assessing passive system reliability
 - Develop an accident progression plant state database
- **Regulatory Technology Development Plan**
 - Prioritize licensing R&D needs for advanced reactor systems

Regulatory Framework – General Design Criteria

- DOE's Advanced Reactor Concepts Technical Review Panel (TRP) identified that:
 - Advanced reactor designers are in need of a regulatory framework that reduces existing regulatory uncertainty for non-LWRs
- Development of General Design Criteria (GDCs) tailored to address non-LWR technology can serve as a first step in such a regulatory framework
- DOE-NRC kickoff meeting held in early August
- Requires close coordination with NRC (recent NRC letter to DOE)
 - NRC would use DOE technical outputs to develop and endorse a new set of GDCs encompassing non-LWRs
- Industry input and insights will be considered as a part of DOE national lab work product development

Regulatory Framework – GDCs

FY14 GDC Development Scope:

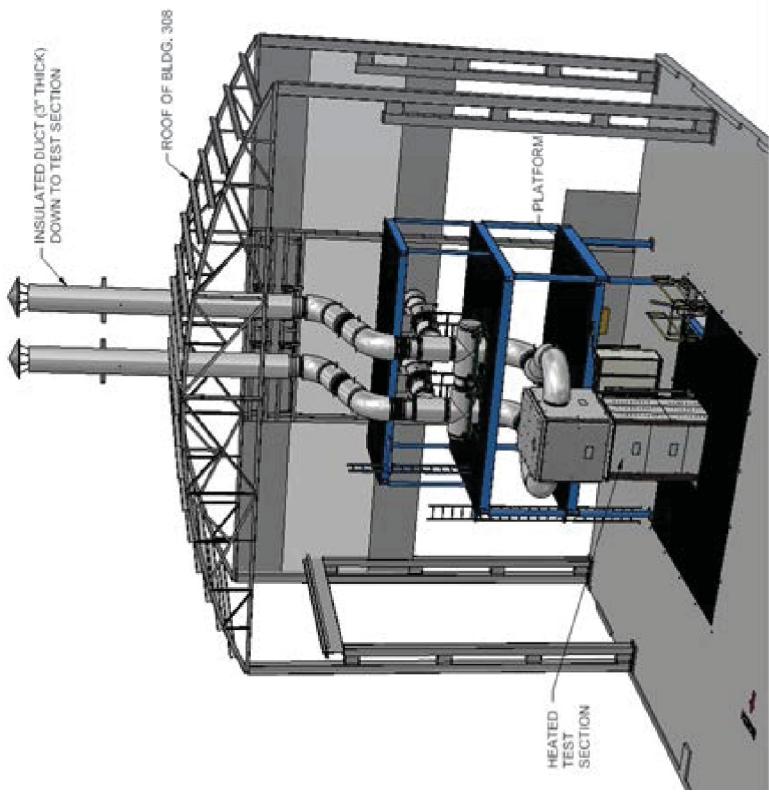
- Complete initial draft set of GDCs (commenced in FY13)
- Incorporate industry and NRC stakeholder input through a series of workshops and public meetings
- Issue a proposed set of non-LWR GDCs for consideration and endorsement by the NRC (i.e. Regulatory Guide, Interim Staff Guidance)

Planned Accomplishment:

- Significantly improved non-LWR stakeholder understanding of this currently uncertain overarching portion of NRC's regulations

NSTF Retrofit – Reactor Cavity Cooling System (RCCS)

- Significant NSTF reconfiguration commenced in late FY12
- Major RCCS construction and initial shakedown testing completed so far in FY13



Planned RCCS Testing in NSTF (FY14 and FY15)

- **Heat Removal Testing Scope**

- FY14: Normal Conditions (incl. weather effects)
 - Carry out tests to evaluate RCCS under normal conditions
- FY14: Accident Conditions (incl. weather effects)
 - Evaluate RCCS under accident conditions – accident power history
- FY15: Testing with partial/full system failures
 - Examine performance with blockages in vent stack and RCCS tubes

- **Planned Accomplishments:**

- Above activities complete the planned 3-year test matrix scope for the RCCS facility:
 - Supports validation of related code work
 - Provides insights and data for passive SSC characterization
 - Supports NRC review and acceptance of this cooling configuration

Key PRA-Related Activities (*FY13*)

- Completed activities within the AdvSMR Program include:
 - Development of a PRA Technical Framework Specification (INL)
 - Identification of Typical Initiating Events for Advanced SMRs (ORNL)
 - Study of Passive Component Evaluation Methods and Knowledge Gaps (ANL)
 - Development of Safety Surrogates for non-LWRS (ORNL)
 - Development of Dynamic Modeling Techniques (SNL)
- NGNP received NRC feedback (“reasonable approach”) on related key concepts:
 - Use of frequency-consequence concept to address regulations
 - Methods for addressing multi-module plant facilities
 - Evaluation of all internal and external event sequences when establishing the licensing basis
 - Consideration of alternatives to core damage frequency risk metric

PRA Framework Next Steps (*FY14 and FY15*)

- The proposed workspace will be for the construction of an analysis and modeling cloud-based framework that will be open for National Laboratories, DOE, NRC, and industry use
 - The probabilistic risk assessment system will focus on advanced SMR issues to demonstrate the technical basis related to safety margins
 - We will build this capability by focusing on available (to the extent possible) open-source tools coupled with existing PRA capabilities
- The overall proposed approach is broken down into three phases
 - Phase 1 – Framework development (completed in FY13)
 - Phase 2 – Prototype development (to be completed in FY14)
 - Addresses the research and development required prior to trial implementation of the key modules that fit into the SRM PRA framework
 - Phase 3 – Case study demonstrations (to be completed in FY15)
 - Addresses the trial use of the SMR PRA concept, demonstrating its usefulness as a design, decision, and optimization tool
 - Specific advanced SMR case studies (using a suitable SMR design) will be performed

Regulatory Technology Development Plan and Initial EP Review

RTDP Scope

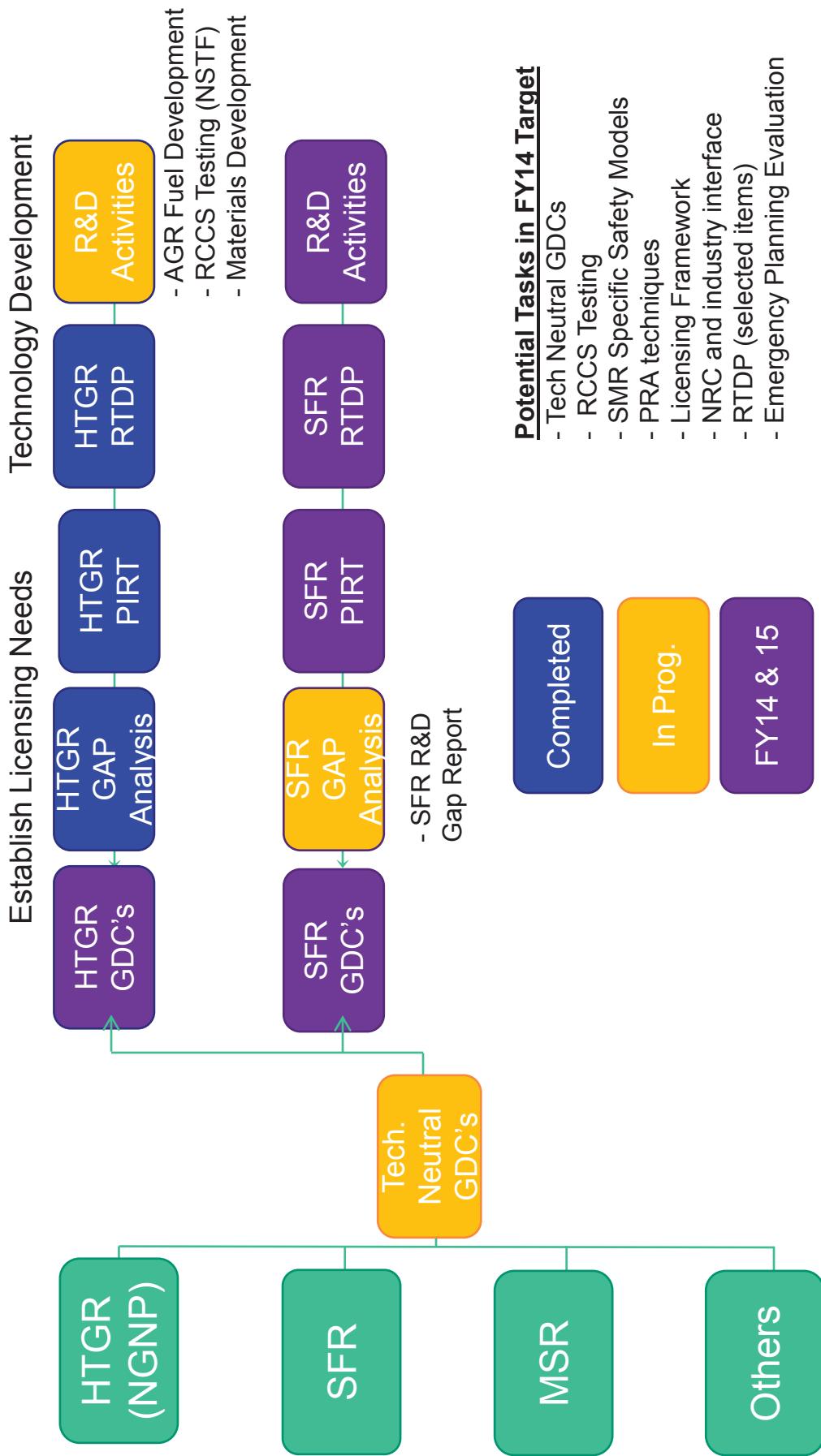
- Incorporate regulatory gap analysis and PIRT experience to prioritize licensing R&D needs for advanced reactor systems
- Integrate licensing efforts with the GDC feedback generated in the Licensing Framework joint initiative with NRC
- Commence the assessment of emergency planning implementation of NRC regulations from SMR perspective.

Planned Accomplishments

- Identifies high-priority licensing-related technology gaps
- Provides insights whether expected SMR EP savings are achievable, improving future focus on necessary technology development activities



BACKUPS



Overview of the Advanced Small Modular Reactor (aSMR) Probabilistic Risk Assessment (PRA) Framework

Curtis Smith

August 2013

www.inl.gov



Topics to be covered

- Goals and vision of the proposed aSMR PRA Framework
- Benefits and motivations
- Aspects of the Framework
- Prototype design elements

The Framework

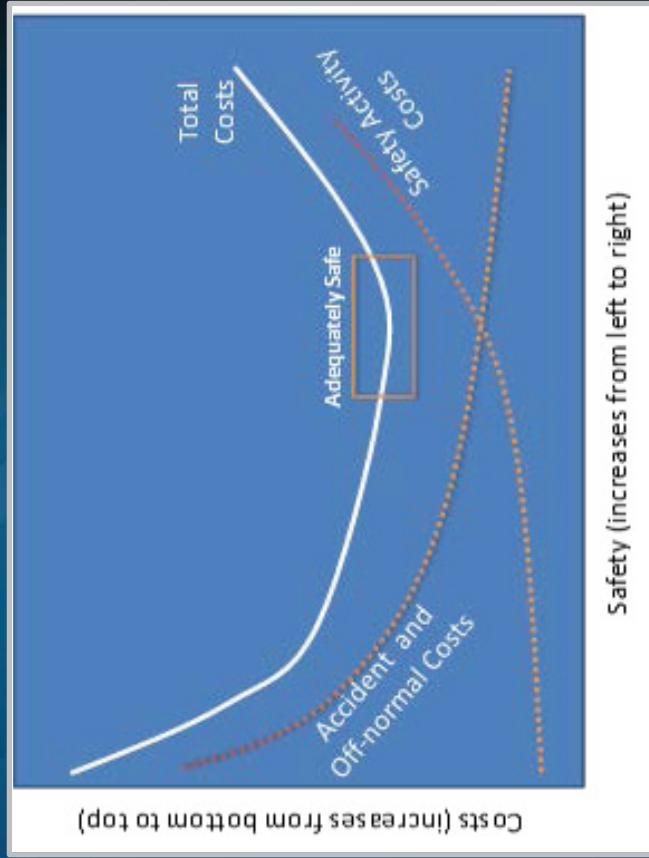
- The aSMR PRA framework has been described in [Small Modular Reactor (SMR) Probabilistic Risk Assessment (PRA) Detailed Technical Framework Specification, INL/EXT-13-28974, April 2013]
- In this framework, the various areas are considered:
 - Probabilistic models to provide information specific to aSMRs
 - Representation of specific SMR design issues such as having co-located modules and passive safety features
 - Use of modern open-source & readily available analysis methods
 - Internal and external events resulting in impacts to safety
 - All-hazards considerations
 - Methods to support the identification of design vulnerabilities
 - Mechanistic & probabilistic data needs to support modeling and tools

Proposed aSMR PRA Framework

- We proposed application & development of methodologies & tools to predict
 - Safety (this is a primary focus)
 - Security
 - Performance
 - Economics
- Goals of assisting in decisions by
 - Developing quantitative methods and tools and the associated analysis framework for assessing a variety of aSMR risks
 - Emphasis on supporting both existing and new quantitative methods for assessing risks

Vision

- Develop a framework for applying modern computational tools to create advanced risk-based methods for identifying design vulnerabilities in aSMRs
- Will require fusion of
 - State-of-the-art PRA methods
 - Advanced 3D visualization
 - High-performance optimization
- Maintain adequate safety in aSMRs



Why a framework?

- Will need a framework to keep everyone on the same page
- We need to predict the **technical basis behind margins** that impact performance measures such as safety
 - These methods & tools will need to use a graded approach both for
 - Short- versus long-term applications
 - Early in design versus during operation
- For the safety case, we will have
 1. Information on the specific aSMR design and operational characteristics
 2. A process to represent (via models) hazards and risks
 3. Evidence that we can control/mitigate hazards/risks to an acceptable level

What unique aspects?

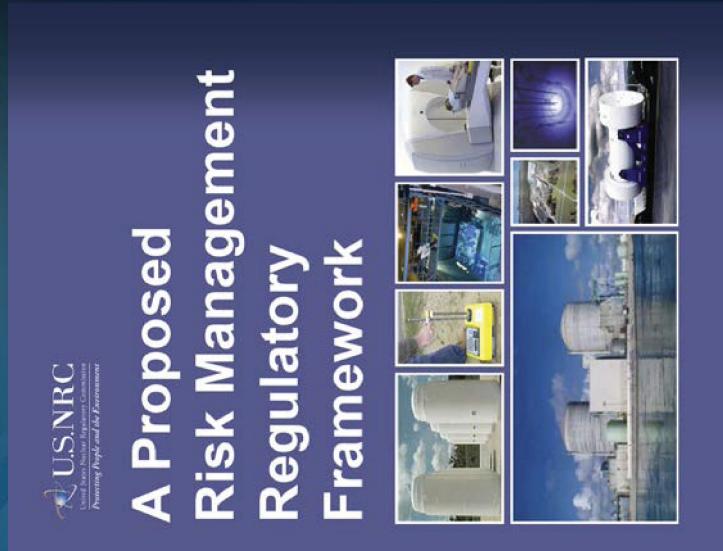
- Holistic view of scenarios across time and hazard types
 - Pre-accident representation in order to improve
 - Boundary condition setting (e.g., more realistic flooding event scenarios)
 - Support for performance measures such as economics
- Ensemble modeling of phenomena
 - Multiple physics models providing multi-physics solutions
- Risk informed decision making support
- Simulation that includes
 - Physical interactions of systems, structures, components, software, and humans
- Parallel and advanced computation techniques

Benefits

- Identify, model and analyze the appropriate physics in an intelligent, scenario-based fashion
 - Avoids limited treatment of dynamic behavior and the need for engineering “fudge factors” in the risk assessment
- Manage the communication and interactions between different physics modeling and analysis technologies
 - Able to represent safety margin, and what drives this, directly
- Provide an analysis platform that can be used to “virtual stress-test” different risk-informed strategies.
- Integrate an ensemble of multiple physics models into a coherent predictive approach to best represent specific scenarios
 - No one model is “correct” and having accurate representation of uncertainty is important to understand safety
- Spatial interactions be represented directly
 - 3D representation of external events (e.g., flooding, fires) would provide enhanced realism to the safety case

Motivations include...

- NRC risk management regulatory framework
 - Provide a vision for a regulatory system 10-15 years in the future
 - The approach should build on the experience of the last 20 years and should be evolutionary rather than revolutionary



The slide features the U.S. NRC logo at the top left. The title "A Proposed Risk Management Regulatory Framework" is centered in large white font. To the right is a collage of six small images showing various nuclear facility scenes: a control room operator, a reactor vessel, a worker in a protective suit, a worker in a yellow vest, a large industrial building, and a cooling tower.

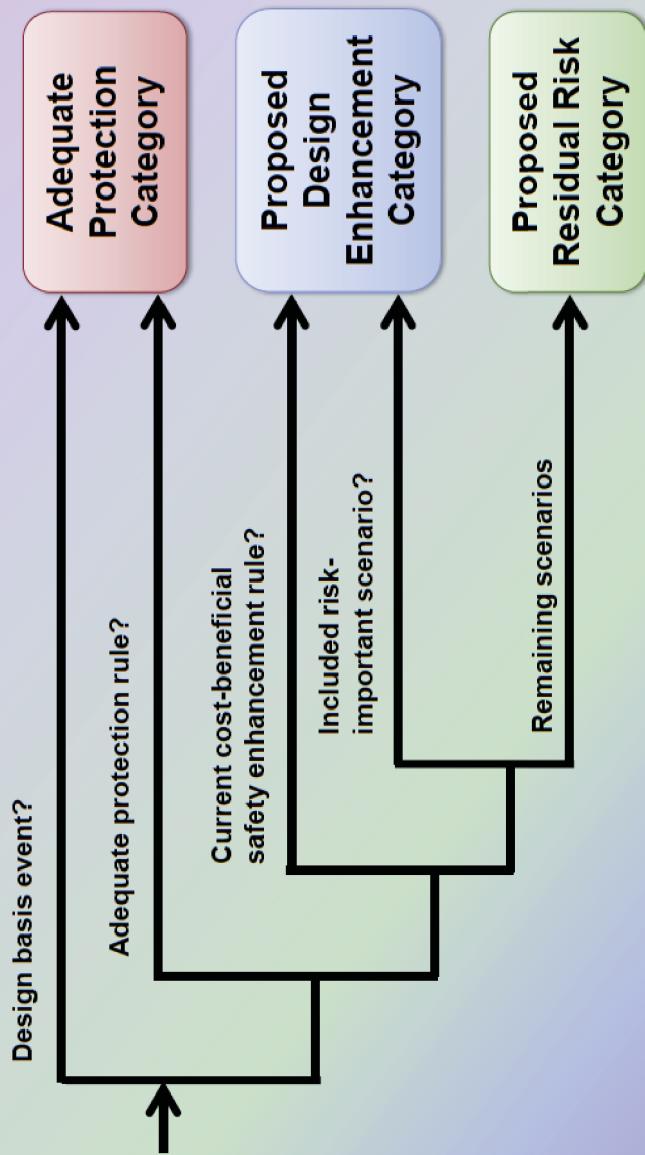
Risk Management Goal

Provide risk-informed and performance-based defense-in-depth protections to:

- Ensure appropriate barriers, controls, and personnel to prevent, contain, and mitigate exposure to radioactive material according to the hazard present, the relevant scenarios, and the associated uncertainties; and
- Ensure that the risks resulting from the failure of some or all of the established barriers and controls, including human errors, are maintained acceptably low

NRC RMRF – An Evolutionary Approach

Proposed Regulatory Framework: Power Reactors



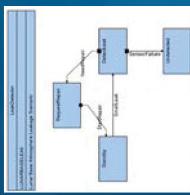
R&D Needed to Identify Design
Enhancement and Residual Risk

Notional approach of the framework (1 of 4)

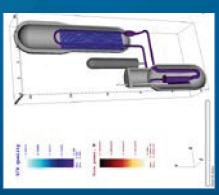
1 Determine risk-based scenarios

Loss of Offsite Power LOSP	Emergency Cooling System - ECS	Containment Cooling System - CCS	#	End State (Phase - PHT)
			1	OK
			2	SMALL-RELEASE
			3	LARGE-RELEASE

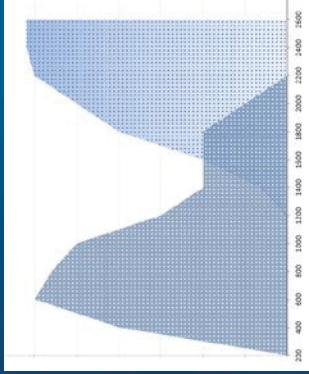
2 Represent plant operation probabilistically



3 Represent plant physics mechanistically

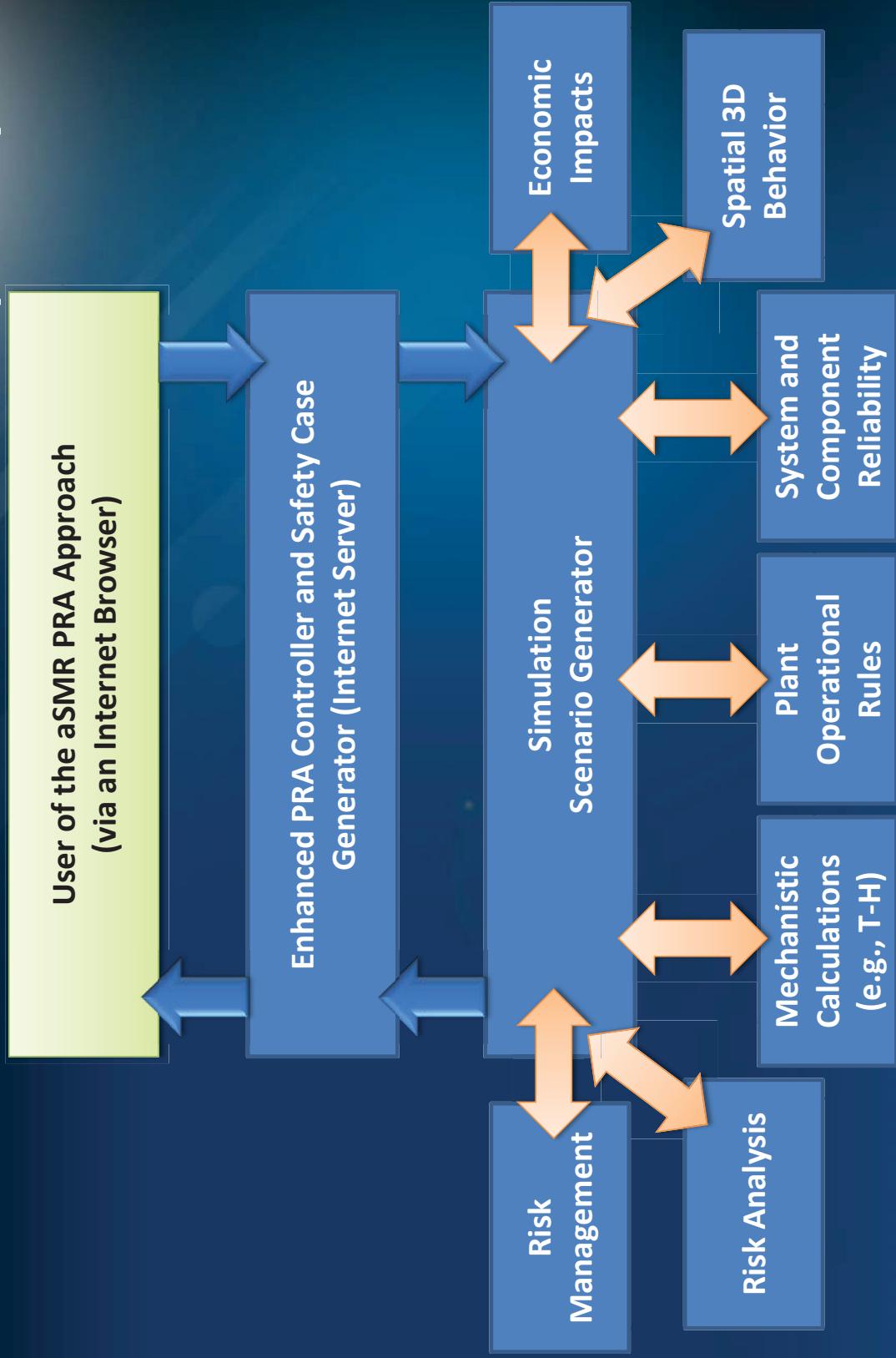


4 Safety margin and uncertainty quantification

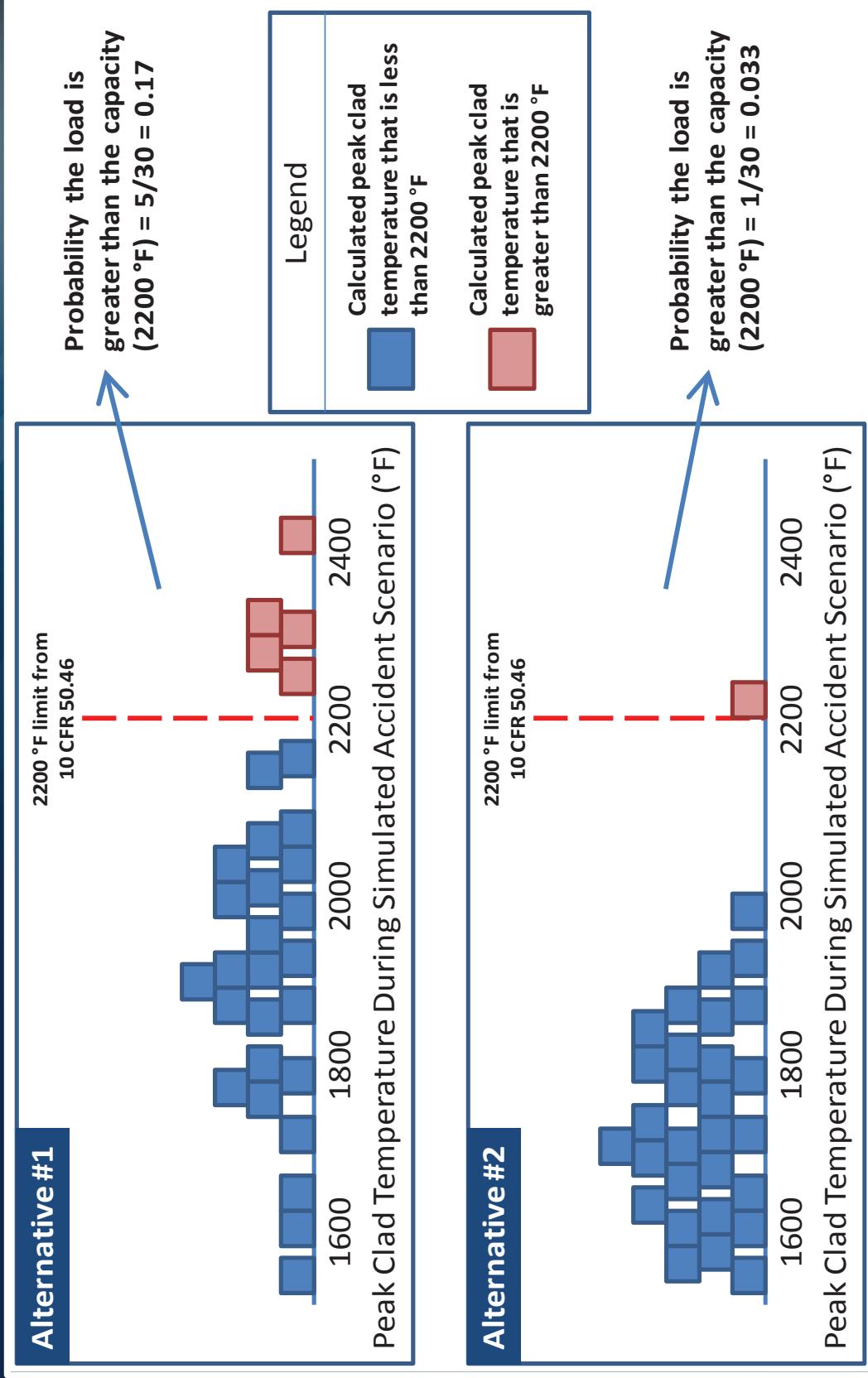


5 Safety case used to support decisions and control safety

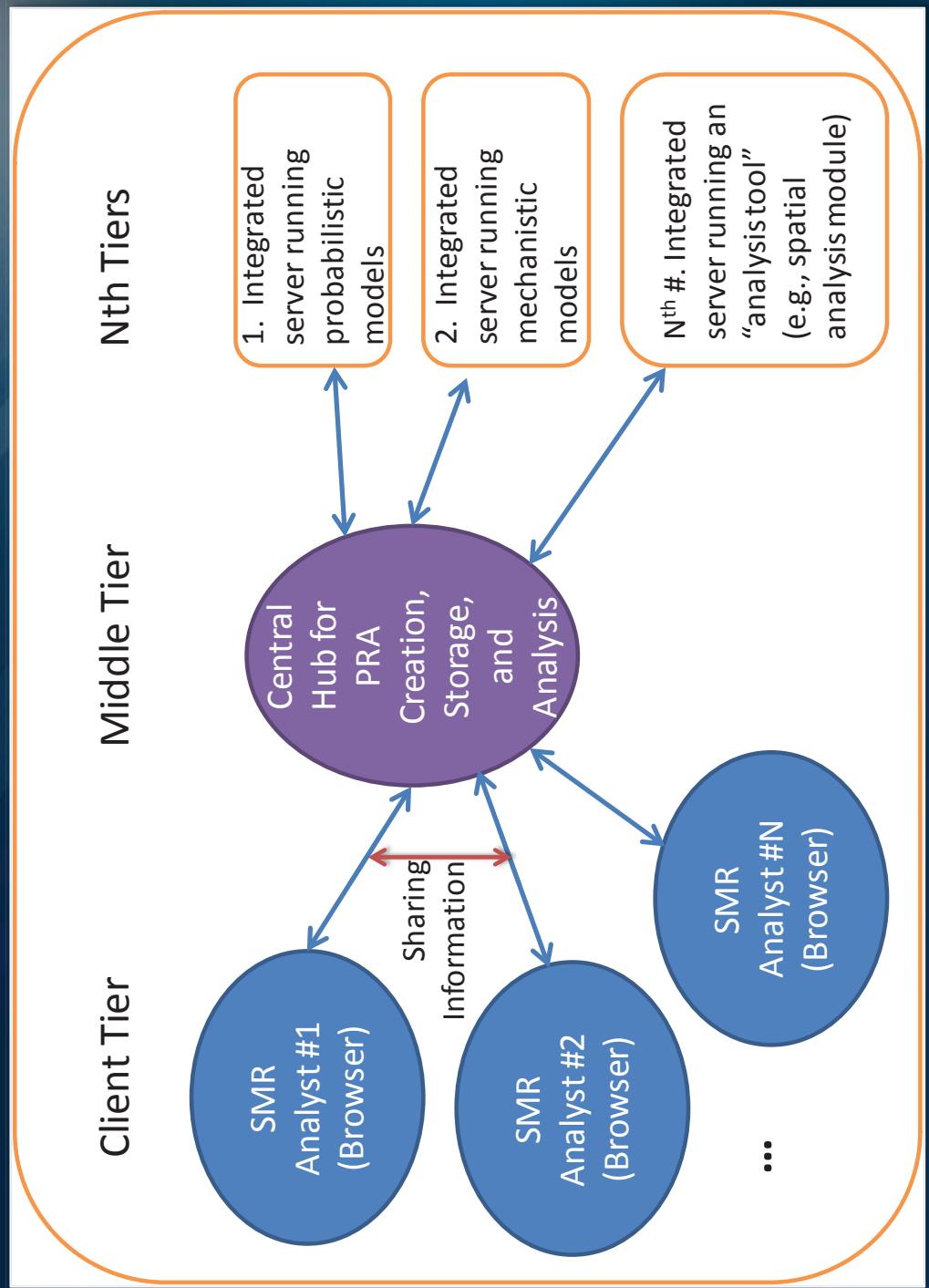
National approach of the framework (2 of 4)



National approach of the framework (3 of 4)



Notional approach of the framework (4 of 4)



Compare proposed approach with existing PRA

Capability	Existing PRA Limitations	Benefits of the Enhanced PRA
Simulation of Accident Scenarios	Limited treatment of dynamic sequence behavior (some discretization used, but this complicates modeling)	Able to capture timing considerations that may affect the safety margin and plant physical phenomena
Safety Margin Evaluation	Margin is not determined, instead discrete end states are decided upon during the model development	Safety margins will be determined directly by coupling mechanistic calculations with probabilistic calculations
Spatial Interactions	Very limited treatment of spatial interactions, mainly in select flooding and fire models	Physics-based 3D environments will capture spatial interactions as part of accident scenarios
Failure Cause Representation	Traditionally, specific failure causes are rolled up into failure models such as fails-to-run or fails-to-start	A robust database of failure causes, mechanisms, and models will be plugged-into the component library such that analysts may pick-and-choose failure modes.
Cloud-based Creation, Analysis, and Storage of Safety Models	Traditionally, safety analysis has been performed by individual risk analysts (or a small team of analysts) with limited sharing and computational support	Multi-discipline, engineering focused teams will be able to share both models and computational resources in order to perform advanced analysis

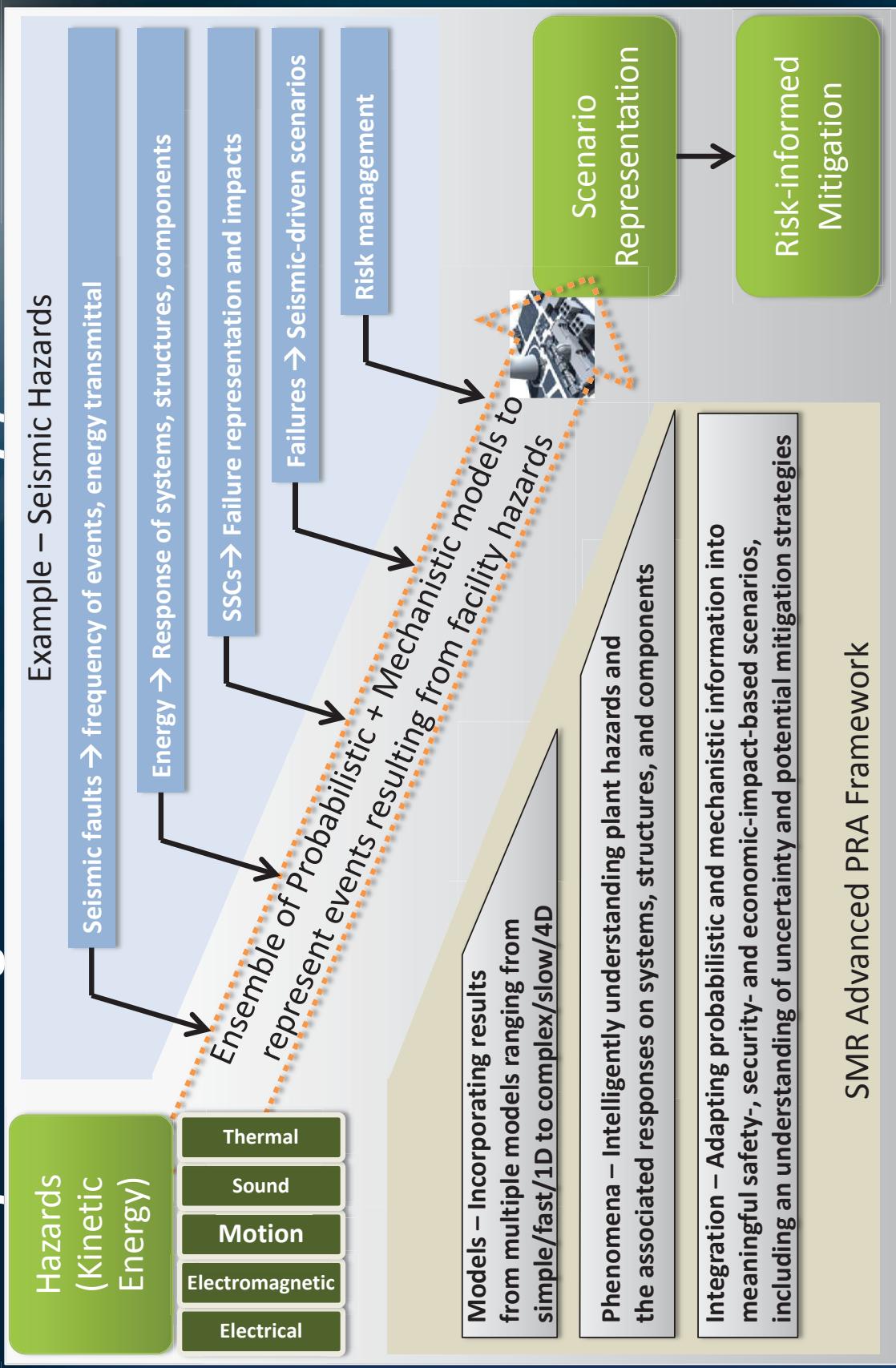
Proposed prototype design

- Prototype described via the following four areas
 - Models
 - 3D representation of the SMR facility for risk analysis
 - *Presentation tomorrow on this topic*
 - Representation of all applicable SMR hazards
 - Phenomena
 - Representation of external hazards, thermal-hydraulics, and other physical processes
 - Representation for passive system behavior
 - Integration of risk results and insights
 - Use of non-traditional safety metrics
 - Risk management to provide Incident Management Guidelines
 - Cloud-based architecture
 - *Presentation tomorrow on this topic*

Analysis relies on advanced capabilities



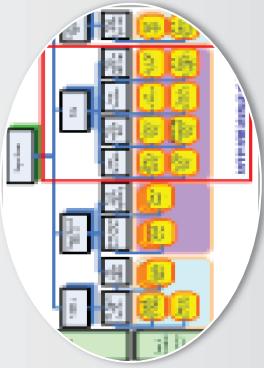
Example using the aSMR PRA approach



Risk management support

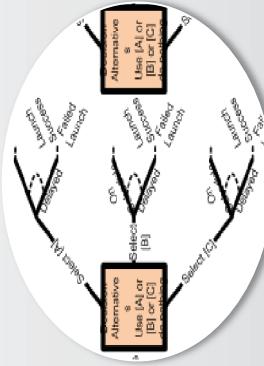
Safety Objectives and Goals

- Qualitative metrics (e.g., redundancy)
- Quantitative metrics (e.g., reliability)
- Analysis requirements and criteria
- Safety decisions



I. Scoping Principles and Goals

- Understand the system
- Normal operation
- Off-normal operation
- Criteria for evaluating alternatives
- Propose design changes when needed



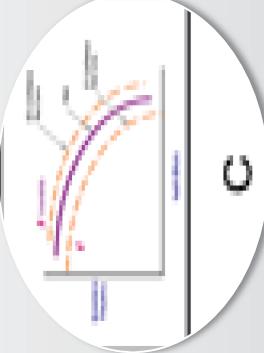
II. Identify and Analyze Hazards

- Address safety requirements
- Model safety hazards, scenarios, and risk
- Perform phenomenological, hardware, and human uncertainty analysis
- Manage uncertainties



III. Support for Implementation

- Provides evidence that system is adequately safe
- Describe how
- Design addresses safety goals
- Safety is allocated
- Safety performance is feasible



Integrated Design and Safety Over the aSMR Lifetime

Cloud architecture

- Ties to various modeling and analysis packages
- Access the model on- or off-line and be able to store copies locally and in the cloud
- Modeling and analysis that is conducted and reviewed in teams of scientists and engineers
- Integrate model, data, and information in order to have a holistic risk analysis and to minimize “stove-piping” the technical models in use
 - Finding the right information at the right time (for analysts, users, and reviewers)
- Synchronize in order to keep everyone on the same page and up-to-date
- Sharing and communication for decision makers, where key insights and uncertainties in the safety case are provided

Conclusions

- We will construct an analysis and modeling cloud-based framework that will be open for National Laboratories, DOE, NRC, and industry
 - It will demonstrate the technical basis related to safety margins
 - It will use available open-source tools coupled with existing PRA capabilities
 - It will consider supporting technologies that are currently available (e.g., 3D environments, multi-processor computers)
- Ultimately, we will need a licensing approach to predict, via a safety case, technical basis behind margins that impact performance measures such as safety

Development of Surrogates for Core Damage Frequency and Large Early Release Frequency for Advanced Small Modular Reactors

June 2013

Prepared by
G. F. Flanagan

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Reactor and Nuclear Systems Division

**DEVELOPMENT OF SURROGATES FOR CORE DAMAGE
FREQUENCY AND LARGE EARLY RELEASE FREQUENCY FOR
ADVANCED SMALL MODULAR REACTORS**

G. F. Flanagan

Date Published: June 2013

Prepared for the
US Department of Energy, Office of Nuclear Energy

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6165
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

	Page
ACRONYMS.....	v
1. INTRODUCTION.....	1
2. BACKGROUND.....	1
3. THE NEED FOR SURROGATES FOR CDF AND CCFP FOR ADVANCED REACTOR DESIGNS	3
4. POSSIBLE SURROGATES FOR ADVANCED REACTORS—LMR.....	4
5. LATENT CANCER FATALITY RISKS.....	5
6. PROMPT FATALITY RISKS	6
7. RECOMMENDATIONS FOR LMR-TYPE REACTORS	7
8. TRISO-FUELED REACTORS	7
9. RECOMMENDATIONS FOR TRISO-FUELED REACTORS.....	8
10. CONCLUSION	8
11. REFERENCES.....	8

ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
aSMR	advanced small modular reactor
CCFP	conditional containment failure probability
CDF	core damage frequency
CLLRPm	conditional large late probability for accident sequence m
CPLF	conditional probability of latent fatality
FHR	fluoride high-temperature reactor
GDC	general design criteria
HTGR	high-temperature gas-cooled reactor
ILR	individual latent risk
LERF	large early release frequency
LF	latent fatalities
LLRF	large late release frequency
LMR	liquid-metal reactor
LOCA	loss-of-coolant accident
LRF	large release frequency
LWR	light water reactor
MHTGR	modular high-temperature gas-cooled reactor
NRC	US Nuclear Regulatory Commission
PRA	probabilistic risk assessment
PRISM	Power Reactor Innovative Small Module
QHO	quantitative health objective
TP	total population
TRISO	tri-structural-isotropic

DEVELOPMENT OF SURROGATES FOR CORE DAMAGE FREQUENCY AND LARGE EARLY RELEASE FREQUENCY FOR ADVANCED SMALL MODULAR REACTORS

1. INTRODUCTION

The current fleet of light water reactors (LWRs) have developed two risk-based surrogates in order to show compliance with the quantitative health objectives (QHOs), which are derived from the US Nuclear Regulatory Commission (NRC) Safety Goal Policy (Ref. 1). The LWR surrogates consist of a preventative component core damage frequency (CDF) and a mitigation component in the form of a containment performance component usually expressed as a conditional containment failure probability (CCFP). In subsequent LWR analyses, these took the form of a CDF and large release frequency (LRF) or large early release frequency (LERF). The purpose of this study is to examine the historical development of the LWR surrogates as contained in SECY-89-102, Regulatory Guide 1.174, and NUREG-1860 and, applying the thought process behind this evolution, to propose surrogates for use in non-LWRs.

2. BACKGROUND

In 1986, the NRC issued the Safety Goal Policy Statement. The statement specified two qualitative safety goals and two QHOs. The two qualitative safety goals are as follows.

- “Individual members of the public should be provided a level of protection from consequences of nuclear power plant operations such that the individuals bear no significant additional risk to life and health.”
- “Societal risks to life and health from nuclear power plants should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.”

The QHOs are as follows.

- “The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.”
- “The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from other causes.”

The early fatality QHO implies that the risk of early fatalities from a reactor should be less than $5 \times 10^{-7}/\text{year}$. The latent fatality goal implies that the risk of fatal cancer to the population in the area (radius of 10 miles) near a nuclear power plant due to its operation should be limited to $2 \times 10^{-6}/\text{year}$.

In order for the NRC staff to determine whether a nuclear power plant meets the QHOs, the Commission issued the following general performance guideline: “Consistent with the traditional defense-in-depth approach and the accident mitigation philosophy requiring reliable performance of containment systems, the overall mean frequency of a large release of radioactive material to the environment should be less than 1 in 1,000,000 per year of reactor operation.”

Former NRC Commissioner James Asselstine suggested in a separate statement the following containment performance criterion: “the mean frequency of containment failure in the event of a severe accident should be less than 1 in 100 severe core damage accidents” in order to ensure proper balance between accident prevention and accident mitigation.

Former NRC Commissioner Frederick Burnthal suggested a CDF of 1 in 10,000 per year of reactor operation and that for future reactors this frequency goal should be reduced further.

Finally, the NRC requested the staff prepare a specific guideline for implementation of the safety goal policy. In June 1990, SECY-89-102, “Implementation of the Safety Goals,” (Ref. 2) was issued. This document stated that the large release guideline, “frequency of a large release of radioactive material to the environment should be less than 1 in 1,000,000 per year of reactor operation,” was more conservative by about one order of magnitude than the QHO, and that this guideline should be applied to all designs independent of the size of containment or character of a particular design approach to the release mitigation function. The SECY proposed that the plant performance objective to meet this guideline be focused on accidental release from the plant and eliminate site characteristics, which is in agreement with Advisory Committee on Reactor Safeguards (ACRS) recommendations.

The SECY suggests partitioning of the release guideline to reflect minimum acceptance criteria for prevention using CDF and mitigation using containment or confinement performance, ensuring a multi-barrier defense-in-depth balance for a reactor design. Based on the probabilistic risk assessments (PRAs) that had been performed to date, a CDF of 1 in 10,000 per year of reactor operation was proposed as the accident prevention allocation. The remainder would be allocated to a conditional containment failure probability or an appropriate deterministic containment performance criterion as the mitigation allocation. It further recognized that evolutionary designs being proposed may result in a lower CDF (1 in 100,000 per year), and therefore a possible 1 in 10 CCFP would be acceptable for such designs. It indicated that a specific subsidiary object might differ from one design class [e.g., LWR and high-temperature gas-cooled reactor (HTGR)] to another. Finally, the SECY stated that the partitioned objectives are not to be imposed as requirements but may be useful as a basis for regulatory guidance.

Regulatory Guide 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” (Ref. 3) restates the CDF of 1 in 10,000 as the basis for measuring whether a change in risks associated with a proposed change in licensing basis will be allowed.

Regulatory Guide 1.174 recognizes that the large release general performance guideline stated in the safety goal policy is the overarching requirement in meeting the QHOs and that CDF and LERF are acceptable methods for meeting the QHO, but direct estimates of large releases can also be used:

“The use of CDF and LERF as the basis for PRA acceptance guidelines is an acceptable approach to addressing Principle 4. Use of the Commission’s Safety Goal QHOs in lieu of LERF is acceptable in principle, and licensees may propose their use. However, in practice, implementing such an approach would require an extension to a Level 3 PRA, in which case the methods and assumptions used in the Level 3 analysis, and associated uncertainties, would require additional attention.”

In Appendix D of NUREG-1860 (Ref. 4), a derivation of the risk surrogates for LWRs was presented that reached the conclusion that a CDF of 10^{-4} /year and a LERF of 10^{-5} /year are acceptable surrogates to the latent and early QHOs, respectively, for the current generation of LWRs.

3. THE NEED FOR SURROGATES FOR CDF AND CCFP FOR ADVANCED REACTOR DESIGNS

The large release guideline defined in the safety goal policy applies to all reactor types and can be demonstrated using a Level 3 PRA. However, this is not in keeping with the ACRS recommendations to eliminate site characteristics in meeting this guideline, and it would be subject to the concerns regarding uncertainties expressed in Regulatory Guide 1.174. In addition, the safety goal policy is directly related to application of risk/benefit design decisions to reduce risks where possible. A Level 3 PRA is an expensive tool to use to assess the risk/benefit of proposed design changes. Thus, the need exists to develop surrogates for advanced small modular reactors (aSMRs) similar to those used by LWRs.

The current use of CDF and LERF (or CCFP) have served this purpose for LWRs. However, as explained below, because of unique features in certain designs, these may not be applicable for some aSMRs. The currently proposed designs for aSMRs are based on two types of fuel designs. The first uses various types of fuel pellets (oxide or metal) in the form of pins clad with metal similar in design to a LWR fuel pin. These include various types of liquid-metal reactors (LMRs). The second type of reactor uses tri-structural-isotropic (TRISO) fuel particles contained in a prismatic graphite matrix or in the form of pebbles. These include the HTGRs and fluoride high-temperature reactors (FHRs). A third type of advanced reactor (homogeneous) uses liquid fuel; these types of reactors differ significantly from heterogeneous designs and pose unique safety and design challenges and are not considered in this report.

The safety goal policy statement is based on the concept of defense-in-depth, which has been a part of the design of nuclear reactors from the beginning. All the aSMRs have a series of physical barriers that make up part of their defense-in-depth design strategy.

In order to have a large release at the site boundary as described in the safety goal policy, it is necessary for the fuel to fail in such a manner as to release significant radioactive fission products into the reactor coolant, which in turn must escape the primary coolant boundary, and then the containment or confinement. This does not assume any emergency response action takes place. Thus, one can assume at least three physical barriers must be breached to have a large early release: (1) fuel coating or clad, (2) primary coolant boundary, and (3) the containment or confinement boundary. All heterogeneous reactor designs, LWR and non-LWR, have the three boundaries listed above. A large release at the site boundary would only occur for beyond-design-basis events since these three boundaries are assumed to be protected for design basis events.

For LWRs, the barrier failure sequence was based on the fact that there was only a small margin associated with cladding failure once the water coolant began to exceed the safety design limits (departure from nucleate boiling or exceeding the critical heat flux). Therefore, it was expected that the first barrier to fail was the fuel cladding, resulting in a release of fission products into the coolant. This was followed by primary system boundary failure due to the stresses associated with the two-phase behavior of the coolant and/or hydrogen release from high-temperature clad interaction with steam. Once the primary system boundary failed, pressure stresses were introduced on the containment boundary that, if high enough, could lead to failure of the containment either rapidly (over stressed) or slowly (increased leak rate). Only then would a large release of radioactivity enter the environment. For loss-of-coolant accidents (LOCAs), a failure of the primary system boundary was the initiating event. If the cladding failed during a LOCA, the radioactive fission products were immediately introduced into the containment.

For advanced reactors such as liquid-metal reactors (LMRs) that have fuel pellets surrounded by cladding acting as a fission product retention barrier, the release of fission products is initiated by failure of the cladding, even though these reactor types have much more margin to failure than LWRs due to the single phase and high boiling point of the coolant, and low-pressure operation. This is followed by failure of the primary system boundary, generally due to high temperatures (creep rupture) or possible energetic releases, followed by failure of the containment or confinement. These latter failures are based on the

severity of the accident. For some types of LMRs (sodium-cooled reactors), containment failure may result from over-pressurization due to coolant chemical reactions.

For the reactors using TRISO fuel, core damage, as postulated in the case of LWR and LMR systems, is highly unlikely since failure of a very large number of small fuel particles would be needed to yield a significant quantity of fission product release. The fuel particles have been shown to have significant robust behavior even at temperatures exceeding 1600°C. In addition to the robust fuel, the HTGR designs generally have a confinement instead of leak-tight containment. This is necessary to prevent sudden overpressure of the containment as a result of a primary system depressurization (e.g., a loss of coolant) accident. The confinement is designed to allow a rapid release of the early pressure pulse containing a limited quantity of fission products (as a result of normal operation) followed by a filtered release. The confinement also acts as a barrier to prevent air or moisture ingress into the reactor following a rapid depressurization, which may have a deleterious effect on the reactor internals and/or fuel coating.

The FHR uses the same robust particle fuel as HTGRs; however, they operate at near atmospheric pressure. FHRs will likely have a leak-tight, low-pressure containment (similar to a LMR) in order to prevent the release of tritium or beryllium during normal operation or as a result of a primary system boundary failure. Over-pressurization of the containment will not likely be an issue for accidents in FHRs.

Thus, for these TRISO-fueled reactors, CDF and LERF are not applicable surrogates to address the LRF requirements associated with safety goal compliance for particle fuel reactors. This position was also taken in the Next Generation Nuclear Plant white paper on PRA (Ref. 5).

4. POSSIBLE SURROGATES FOR ADVANCED REACTORS—LMR

For advanced reactors such as LMRs that have fuel pins with metal cladding separating the fuel from the coolant, the concept of CDF could be interpreted in much the same manner as for LWRs, and therefore, CDF is an applicable surrogate. The issue then becomes the following: Is a frequency of $10^{-4}/\text{year}$, the value suggested for LWRs, the appropriate value for LMRs? LMRs operate at lower pressures, and the coolants have significantly better heat conductivity and operate far below the boiling point compared to LWRs, resulting in significantly larger margins to cladding failure compared to LWRs. LMR designers have considered using a CDF goal of CDF of $10^{-5}/\text{year}$ in order to meet the Commission's expectation (Ref. 6) that advanced reactors should have at least the equivalent level of safety as the current LWRs and will provide enhanced margins of safety. Current LMR designs can achieve a $10^{-5}/\text{year}$ CDF based on studies performed on the Power Reactor Innovative Small Module (PRISM) and sodium advanced fast reactor passively safe designs (Ref. 7). Thus, setting a goal of CDF of $10^{-5}/\text{year}$, the preventative component requirement can more than adequately be met, even allowing for uncertainty due to the lack of operational data.

If this value is used as the preventative component in meeting the QHO as suggested in SECY-89-102, then the CCFP could be reduced to $10^{-1}/\text{year}$ in order to meet the goal of $10^{-6}/\text{year}$ large release and yet retain an appropriate ratio of prevention to mitigation. Since LMR containments are generally not the high pressure leak-tight systems found in typical LWRs, reducing the CCFP by an order of magnitude will allow flexibility in the design of LMR containments, yet retain a reasonable ratio of prevention vs mitigation, as suggested in SECY-89-102. "The Commission has no objection to the use of the 10^{-1} CCFP objective for the evolutionary design in the manner described above." Thus, the large release performance guideline ($10^{-6}/\text{year}$) can be met by the LMR using 10^{-5} CDF and a CCFP of 10^{-1} .

NUREG-1860 (Ref. 4) suggested that CDF could be a direct surrogate for the latent cancer death QHO when applied with open containment for the existing fleet of LWRs. The following derivation, based on a similar derivation from NUREG-1860, indicates that a CDF of $10^{-5}/\text{year}$ for an LMR could be used as a

surrogate for the latent cancer QHO provided the largest conditional probability of latent fatalities (CPLFs) within a 10-mile radius for internal initiators is $< 4 \times 10^{-2}$. In order to establish this case, a LMR Level 3 PRA is needed to ensure a CPLF $< 4 \times 10^{-2}$ can be achieved. The following derivation as presented in Sect. 5 from NUREG-1860 Appendix D was used to justify this suggestion.

5. LATENT CANCER FATALITY RISKS

The risk to the population from cancer “resulting from all other causes” is taken to be the cancer fatality rate in the United States, which is about 1 in 500 or 2×10^{-3} /year. The safety goal criteria of one-tenth of one percent of this figure implies that the risk of fatal cancer to the population in the area near a nuclear power plant due to its operation should be limited to 2×10^{-6} /reactor year.

$$\text{i.e.: } 1/10 * 1\% * 2 \times 10^{-3} = 2 \times 10^{-6}.$$

The “area” is understood to be an annulus of 10-mile radius from the plant site boundary. The cancer risk is also determined on the basis of an average individual latent risk (ILR), that is, by evaluating the number of latent cancers (societal risk) due to all accidents to a distance of 10 miles from the plant site boundary, weighted by the frequency of the accident, dividing by the total population (TP) to 10 miles, and summing over all accidents. This implies

$$\text{ILR} = \sum_1^M [(\text{LF}_m * \text{LLRF}_m)/\text{TP}(10)], \quad \text{Equation 1}$$

where LF_m = number of latent cancer fatalities within 10 miles conditional on the occurrence of the accident sequence “m” and

LLRF_m = frequency/year of a release leading to a dose to an offsite individual TP(10) = total population to 10 miles.

The number of latent fatalities (LF_m) expected to occur for a certain population TP(10) given an accident is expressed as follows:

$$\text{LF}_m = \text{CPLF}_m * \text{TP}(10), \quad \text{Equation 2}$$

where CPLF_m = conditional probability of an individual becoming a latent fatality for an accident sequence “m”.

Therefore, the CPLF is

$$\text{CPLF}_m = \text{LF}_m/\text{TP}(10). \quad \text{Equation 3}$$

Consequently, the ILR is (combining Equations 1 and 3)

$$\text{ILR} = \sum_1^M \text{CPLF}_m * \text{LLRF}_m. \quad \text{Equation 4}$$

It can be shown that if a plant’s CDF is 10^{-4} /year or less, the latent fatality QHO is generally met. This acceptance can be demonstrated numerically using the results of probabilistic consequence assessments carried out in Level 3 PRAs as follows:

- 1) Assuming that one accident sequence “m” dominates the latent fatality risk and the LLRF.
- 2) Assuming the accident sequence dominating the risk is the worst case scenario:
 - a large opening in the containment and/or
 - an unscrubbed release that occurs after effective evacuation of the surrounding population (i.e., no early fatalities occur).

- 3) Assuming that the accident occurs in an open containment, the conditional probability of large late release (CLLRP_m) is 1.0; that is,

$$\text{LLRF}_m = \text{CDF}_m * \text{CLLRP}_m \quad \text{Equation 5}$$

$$\text{LLRF}_m = \text{CDF}_m * 1.0 .$$

Therefore,

$$\text{ILR}_m = \text{CPLF}_m * \text{CDF}_m . \quad \text{Equation 6}$$

- 4) Using results from NUREG-1150 (Table 4.3-1) for the Surry PRA, the largest CPLF (within 10 miles) for internal initiators is 4×10^{-3} .

The calculated CPLF values are very uncertain and; therefore, the approach adopted was to select a conservative estimate of CPLF. A CPLF value was therefore selected from the high consequence-low frequency part of the uncertainty range. This CPLF value corresponds to a large opening in containment and a very large release. It is therefore consistent with the worst case assumptions for accident scenario “m.”

Using the above value of CPLF and assuming a CDF goal of $10^{-4}/\text{year}$, an estimate of the ILR can be made using Equation 6:

$$\text{ILR}_m = (4 \times 10^{-3}) * (10^{-4}) = 4 \times 10^{-7}/\text{year} .$$

The ILR corresponding to a $\text{CDF}=10^{-4}/\text{year}$ is less than the latent cancer QHO of $2 \times 10^{-6}/\text{year}$ by a factor of about five. Using a CDF goal of $10^{-4}/\text{year}$ will generally ensure that the latent cancer QHO is met. Therefore, a CDF of $10^{-4}/\text{year}$ is an acceptable surrogate for the latent cancer QHO for LWRs.

Since it is recommended that LMR designers consider using a CDF goal of $10^{-5}/\text{year}$ as opposed to using $10^{-4}/\text{year}$ for LWR, which is used in the derivation above, the latent fatality QHO requirement can more than adequately be met if the LMR Level 3 PRA conditional probability of latent fatalities (within a 10-mile radius) for internal initiators is $< 4 \times 10^{-2}$.

6. PROMPT FATALITY RISKS

NUREG-1860 also suggested that the LERF is a surrogate for prompt fatality, which is the more conservative of the QHOs. The definition of LERF used by the staff is “a large early release as a significant unmitigated release from containment before effective evacuation of the close-in population such that there is a potential for prompt health effects” (Ref. 8).

The PSA Applications Guide (Ref. 9) introduced the term LERF and included the following definition for large early release:

- unscrubbed containment failure pathway of sufficient size to release the contents of the containment (i.e., one volume change) within 1 hour, which occurs before or within 4 hours of vessel breach; or
- unscrubbed containment bypass pathway occurring with core damage.

Safety analysis of passively safe LMRs indicates that accident progression is slow compared to LWRs, and the systems operate at near atmospheric pressure. Thus, there is no driver for early containment failure; consequently, the concept of LERF as defined above is not applicable to LMR designs (Ref. 10).

Therefore, the use of LERF as a surrogate for the prompt fatality QHO for an LMR is not applicable. This is consistent with SECY-13-0029, which indicates the LRF will continue to be used for new reactors while LERF will be used for existing plants.

7. RECOMMENDATIONS FOR LMR-TYPE REACTORS

For a LMR, a CDF of 10^{-5} /year is achievable with current designs (Refs. 7 and 10) and when combined with a CCFP of 10^{-1} more than adequately addresses the guideline in SECY-89-102. This also meets the NRC-stated expectation that advanced nuclear reactors demonstrate a level of safety equal to or better than the current LWRs (see Commissioner Burnthal's comments in Sect. 2 and reference 6). Using the methodology in Appendix D of NUREG-1860, and a CDF of 10^{-5} /year, an LMR will meet the Safety Goal QHO for latent fatalities if future Level 3 LMR PRAs show that the conditional probability of latent fatality is $<4.3 \times 10^{-2}$ /year within a 10-mile radius. A CDF value of 10^{-5} /year will therefore meet the latent fatality QHO with a large margin, which would allow for uncertainties such as would be expected for reactors where little operating experience exists. For LMRs, the concept of an LERF may not apply because of increased margins to coolant boiling, better coolant thermal conductivity, and low-pressure operation. Instead, it is recommended that CCFP (or an appropriate deterministic containment performance requirement) be used for the mitigation portion of defense in depth as suggested in SECY-89-102. The CCFP used would be 10^{-1} , allowing the designer more flexibility in containment design. This is in accordance with SECY-89-102.

8. TRISO-FUELED REACTORS

For TRISO-fueled reactors, the concept of CDF does not apply [non-LWR PRA standard (Refs. 5, 11, and 12)]. Thus, an alternative surrogate is needed if one is to avoid the need for the introduction of site characteristics along with large uncertainties as would occur if using a Level 3 PRA as part of the information needed to comply with the safety goal policy statements.

Based on HTGR and FHR designs, there are three physical barriers to release of fission products: the robust TRISO fuel coating, the primary coolant boundary, and containment or confinement. In order for an accident to progress to a state where there is a potential for significant release of fission products, the primary system would need to be breached, resulting in a loss of cooling capability which, in turn, could lead to some fuel particles reaching fuel temperatures in excess of 1600°C , or ingress of air or water that may result in fuel damage due to degradation of the fuel coating. Based on accident analysis to date, no release is possible if the primary system boundary remains intact (Ref. 12). Thus, the designs need to prevent such a breach. However, should a breach occur, the reactor systems are designed to remove heat using passive systems and prevent fuel damage. Furthermore, if the primary system boundary is breached, there will likely be small amounts of radioactivity released resulting from normal operations. Thus, even after breach of the primary system, there will not be sufficient release to challenge the performance guideline of 10^{-6} /year for large release to the environment. The primary mitigation barrier after failure of the primary system boundary is the fuel particle and the confinement or containment. In analyses to date, significant fuel damage is not expected until the particle temperature reaches 1600°C (Ref. 13). Safety analysis of the modular high temperature gas-cooled reactor (MHTGR) indicates that for most accidents, including air or water ingress events following breach of the primary coolant boundary, the fuel temperature remains below 1600°C . Based on the data developed for the HTGR, the preventive design allocation to meet the performance guideline would be 10^{-4} /year for primary system boundary failure. The remaining conditional failure mitigation allocation 10^{-2} would be split between preventing releases from the confinement and/or preventing damage to the fuel coating which might result in significant fuel damage. To date, the knowledge gained from TRISO fuel tests and limited operational experience with TRISO fuel indicates that if fabrication quality standards are met, the probability of failure of a large number of TRISO fuel particles resulting in a large radioactive release to the environment is orders of magnitude below 10^{-2} given a failure of primary system boundary (Ref. 13). Thus, the performance guideline can be met with large margin by the fuel alone, even if confinement is not credited. The mitigation performance measure would be directly attributed to fuel fabrication quality.

9. RECOMMENDATIONS FOR TRISO-FUELED REACTORS

For TRISO fuel reactors (HTGR and FHR), the concept of using a balance (prevention to mitigation) of defense-in-depth barriers to achieve the safety goal performance guideline as stated in SECY-89-102 results in an allocation of an achievable (based on past HTGR safety analyses - Ref. 12) primary boundary failure frequency of 10^{-4} /year as the preventative allocation and relying on either fuel integrity (achieved by a high level of fuel fabrication quality objectives) and/or confinement barrier performance for the remaining 10^{-2} mitigation component. The decision as to the allocation attributed to fuel coating integrity or confinement /containment performance would be a design decision allowing considerable flexibility in containment/confinement design performance criteria.

The use of CDF or LERF are not applicable to a TRISO-fueled reactor, and thus, a direct link between the recommended surrogates to the QHOs following the methodology of Appendix D of NUREG-1860 is not applicable to these designs.

In lieu of a surrogate, the designer can use a direct calculation of prompt fatalities and latent cancer fatalities derived from a Level 3 PRA analysis along with appropriate site characteristics to show direct compliance with the QHOs per Regulatory Guide 1.174.

10. CONCLUSIONS

The above-recommended surrogates apply to two forms of advanced reactors—those with fuel similar in form to LWRs and those using TRISO fuel. It may be possible to extend this concept of development of a preventative surrogate and a mitigation surrogate in a technology neutral framework that when combined can be used to meet the overall Safety Performance Guideline of 10^{-6} /year for all currently conceived aSMRs. However, recently the Department of Energy and NRC have embarked on an effort to develop technology neutral general design criteria (GDC) that will define the boundaries that will be protected and further focus on defense-in-depth approaches for advanced systems. In order to remain consistent with this effort, it seems prudent not to further define technology neutral surrogates until the GDCs are defined. This report as completed, thus far, can provide useful information to the technology neutral GDC task. Once technology neutral GDCs are defined, a consistent set of technology neutral surrogates can be developed.

11. REFERENCES

1. “Safety Goals for the Operation of Nuclear Power Plants; Policy Statement,” *Federal Register*, Vol. 51 (51 FR 30028), US Nuclear Regulatory Commission, August 21, 1986.
2. “Implementation of the Safety Goals,” SECY-89-102, US Nuclear Regulatory Commission, June 1990.
3. “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, Revision 1, US Nuclear Regulatory Commission, November 2002.
4. “Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing,” NUREG-1860, U.S. Nuclear Regulatory Commission, December 2007.
5. “Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper,” INL/Ext-11-21270, Idaho National Laboratory, Idaho Falls, ID, September 2011.

6. "Regulations of Advanced Power Plants; Statement of Policy," *Federal Register*, 51 FR35461, July 12, 1994.
7. General Electric Advanced Nuclear Technology, *PRISM Preliminary Safety Information Document*, Appendix A, "PRISM Preliminary Probabilistic Risk Assessment," GEFR-00793, UC-87Ta, December 1987.
8. "History of the Use and Consideration of the Large Release Frequency Metric by the U.S. Nuclear Regulatory Commission," SECY-13-0029, US Nuclear Regulatory Commission, August 15, 1996.
9. "PSA Applications Guide," EPRI TR-105396, August 1995.
10. M. Denman, J. LaChance, T. Sofu, G. Flanagan, R. Wigeland, and R. Bari, *Sodium Fast Reactor Safety and Licensing Research Plan—Volume 1*, SAND2012-4260, Sandia National Laboratories, Albuquerque, NM, May 2012.
11. The American Society of Mechanical Engineers, Committee on Nuclear Risk Management, *Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plants*, Draft, October 2008.
12. P. M. Williams et al., *Draft Pre-application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG-1338, US Nuclear Regulatory Commission, 1989.
13. R. P. Wichner and S. J. Ball, *Potential Damage to Gas-Cooled Graphite Reactors Due to Severe Accidents*, ORNL/TM-13661, Oak Ridge National Laboratory, Oak Ridge, TN.

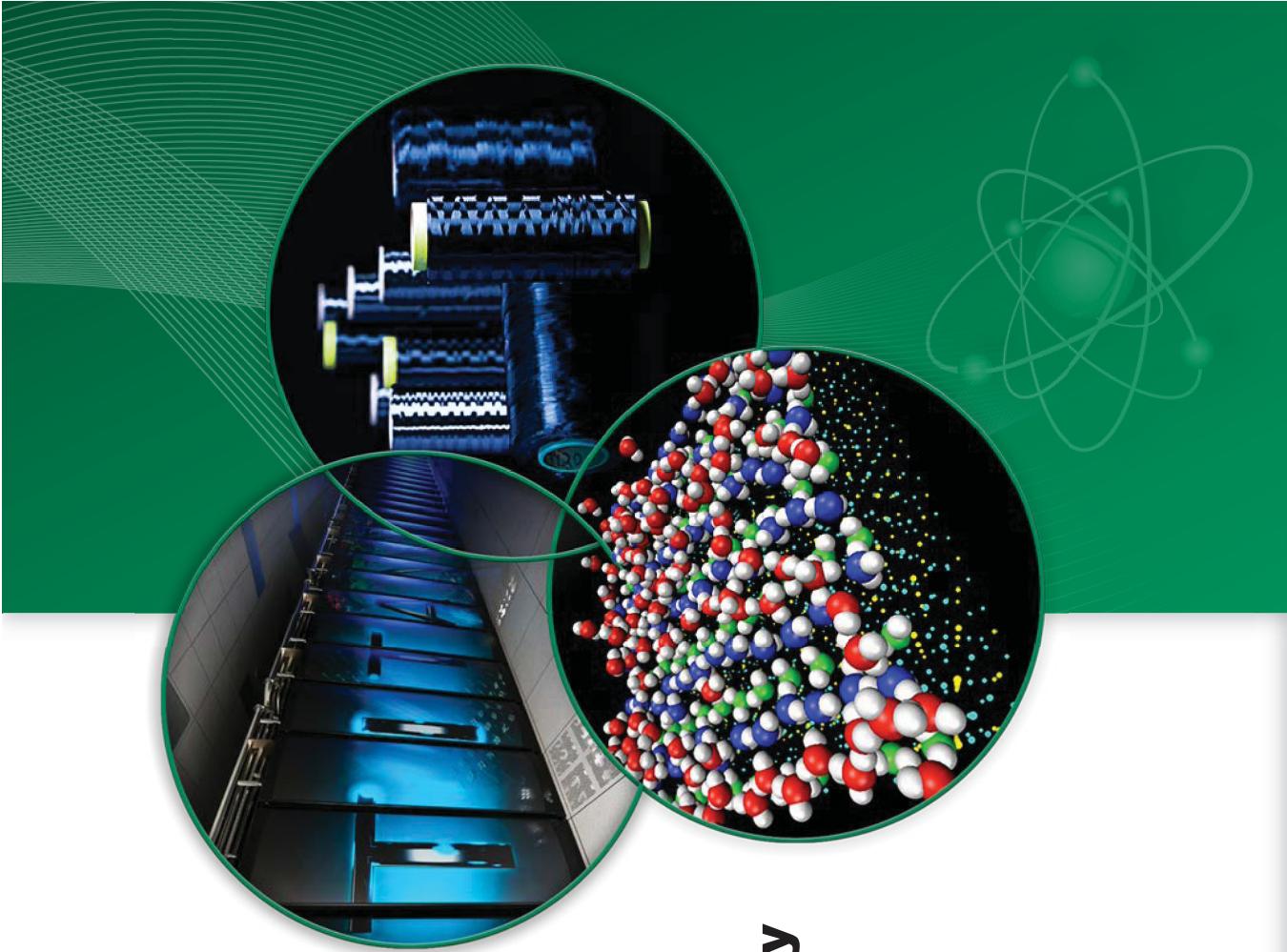
Identification of Initiating Events for aSMRs

Michael D. Muhlheim

Oak Ridge National Laboratory

Advanced SMR PRA Framework
Technical Exchange Meeting

August 21-22, 2013



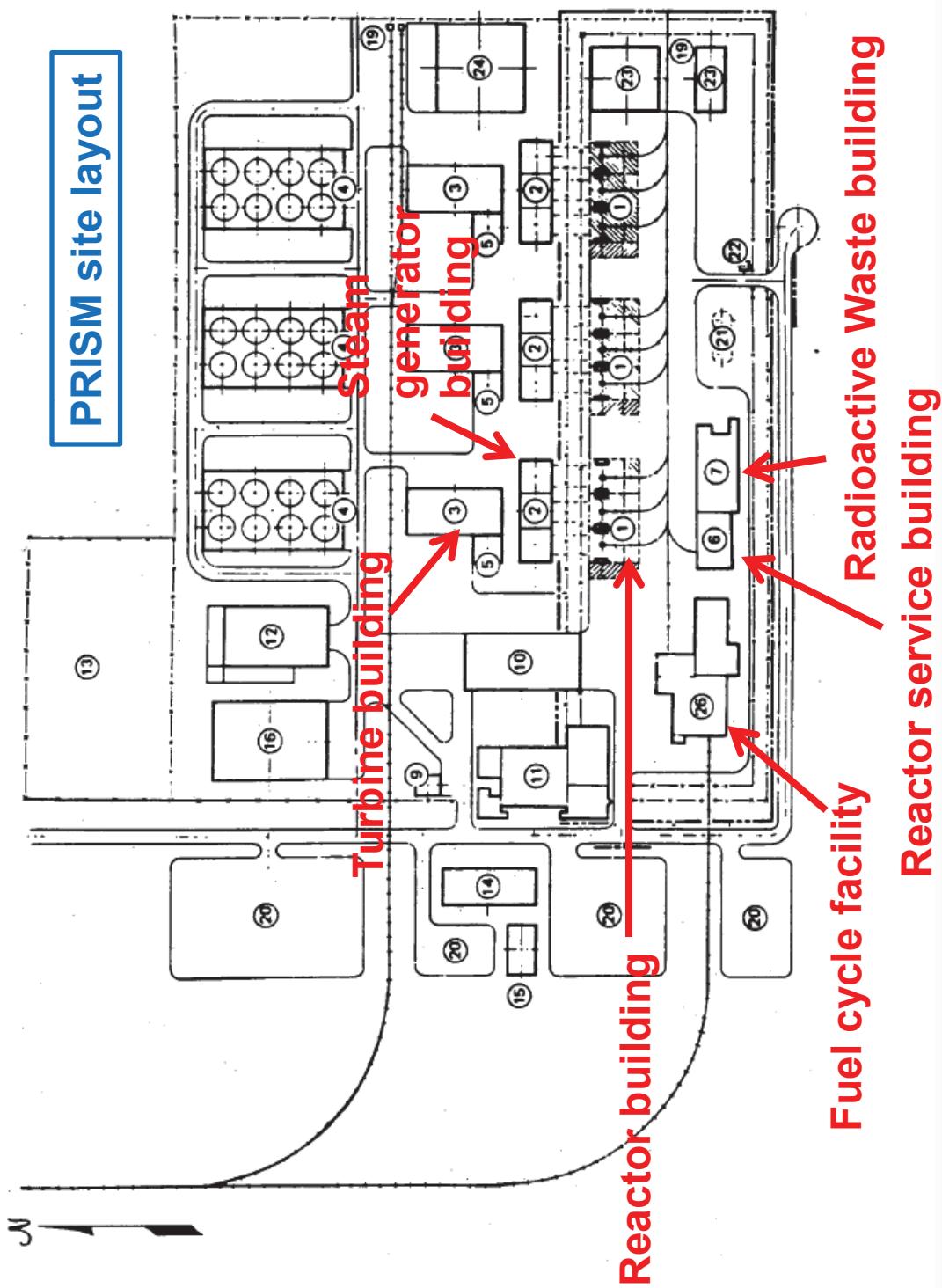
Presentation Outline

- Scope
- Systematic Review Process
- Components of that Process
- Grouping of Initiating Events (IEs)
- Special Issue—Integrated Site Risk
- Conclusions and Insights

The Purpose of this Task is to Develop a Generic Set of Potential IEs for an aSMR under DOE-NE's aSMR R&D Program

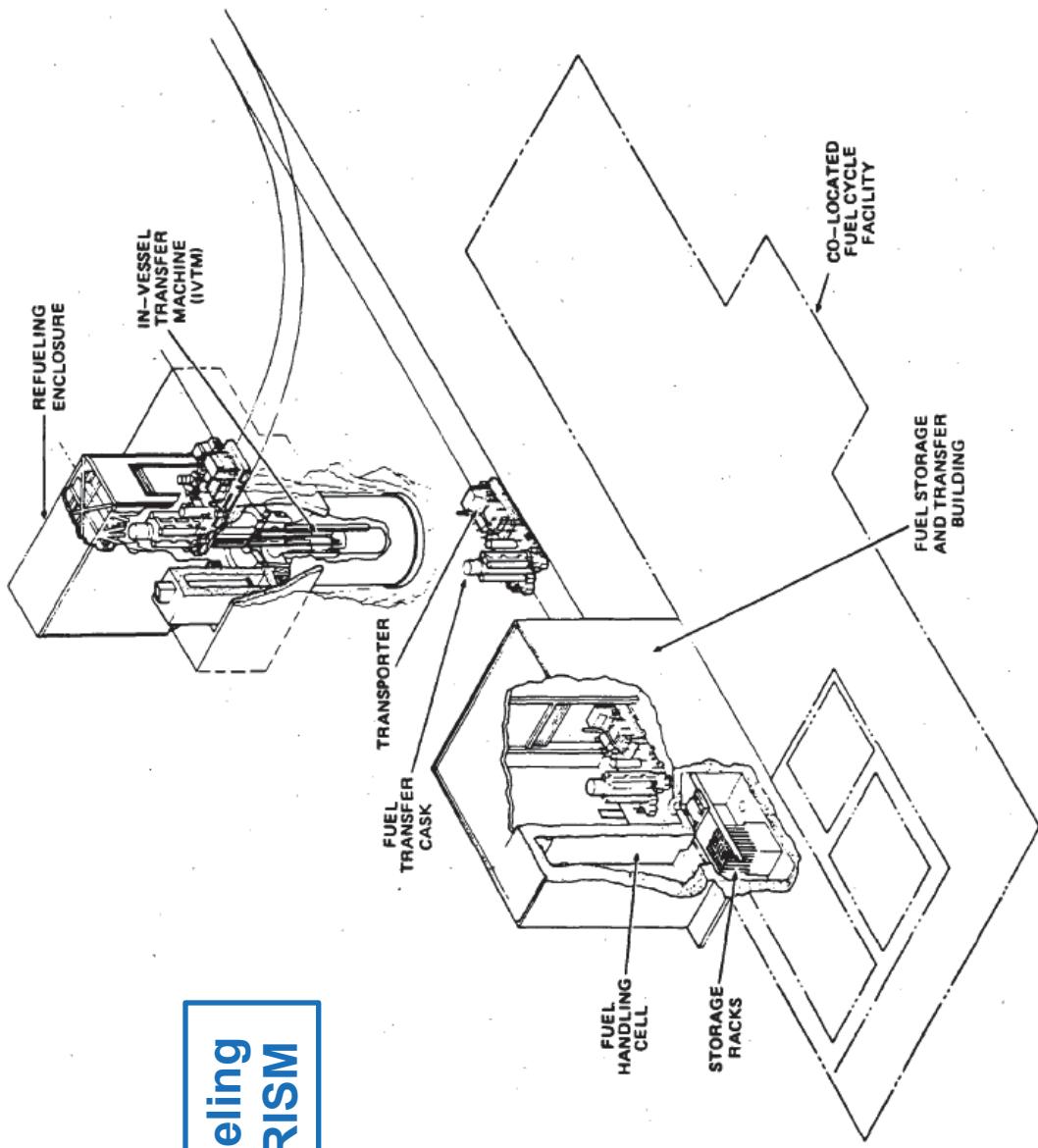
- IEs are the beginning points in the accident sequences that encompass the effects of all realistic and physically possible potential accidents involving irradiated components, reactor fuel, or the reactor core, and include potential radioactive releases.
 - IEs can be internally or externally generated.
- The process used to identify IEs evaluates all sources of radiological risk to health and safety and to the environment
 - Reactor core and connected systems,
 - Spent/used fuel storage and handling,
 - Dry cask storage, and
 - Radiological and nonradiological systems.
- Accidents resulting from purposeful human-induced security threats (e.g., sabotage, terrorism) and risks associated with accidental radiological exposures to on-site personnel are beyond the scope of this review.
- Results are provided in ORNL/LTR-2013-230, *Identification of Initiating Events for aSMRs*, June 2013.

Sources of Radioactive Material are not Centrally Located as in Large LWRs



Refueling at aSMRs is Very Different Than Refueling at Large LWRs

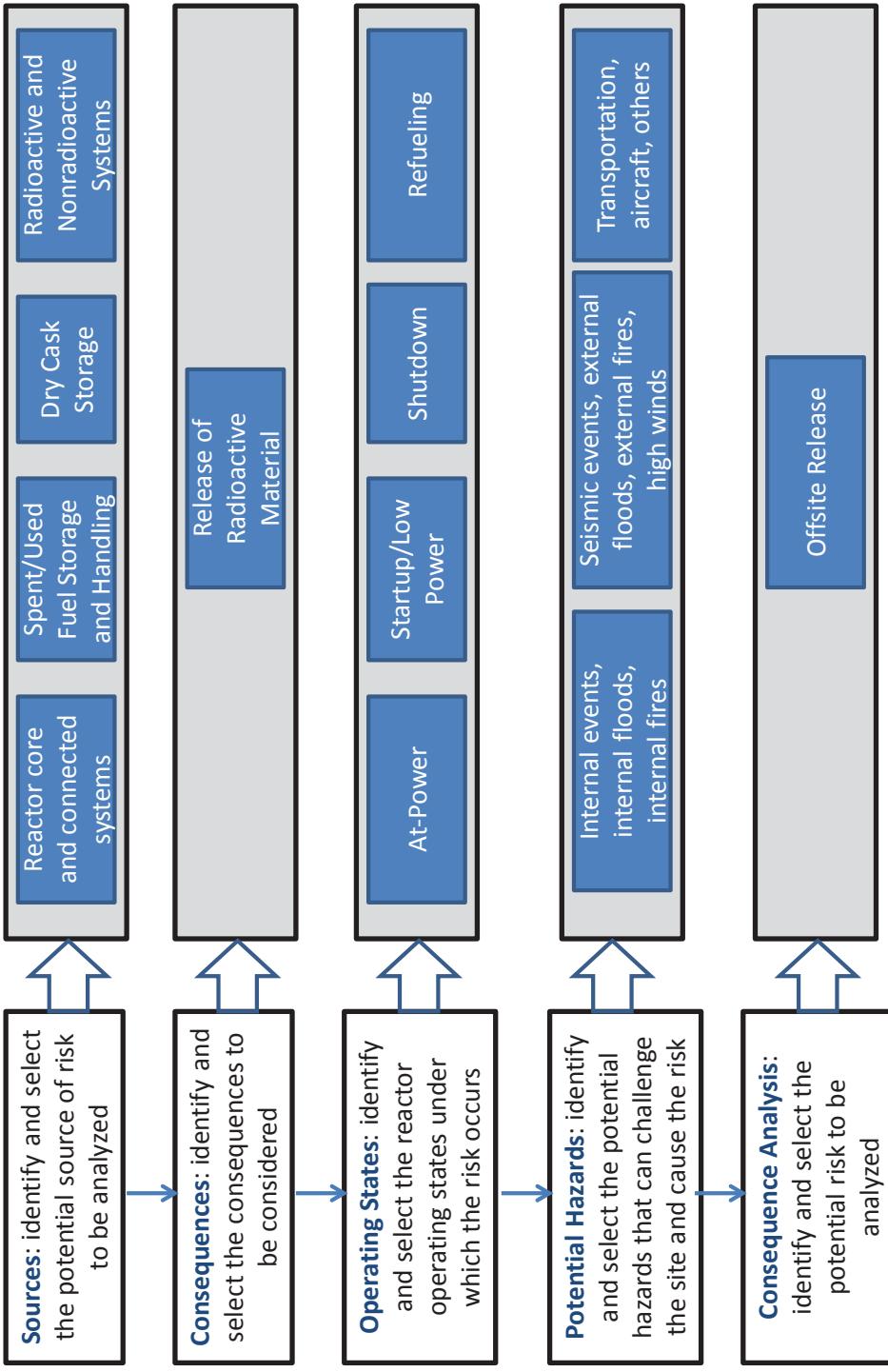
Reactor refueling system at PRISM



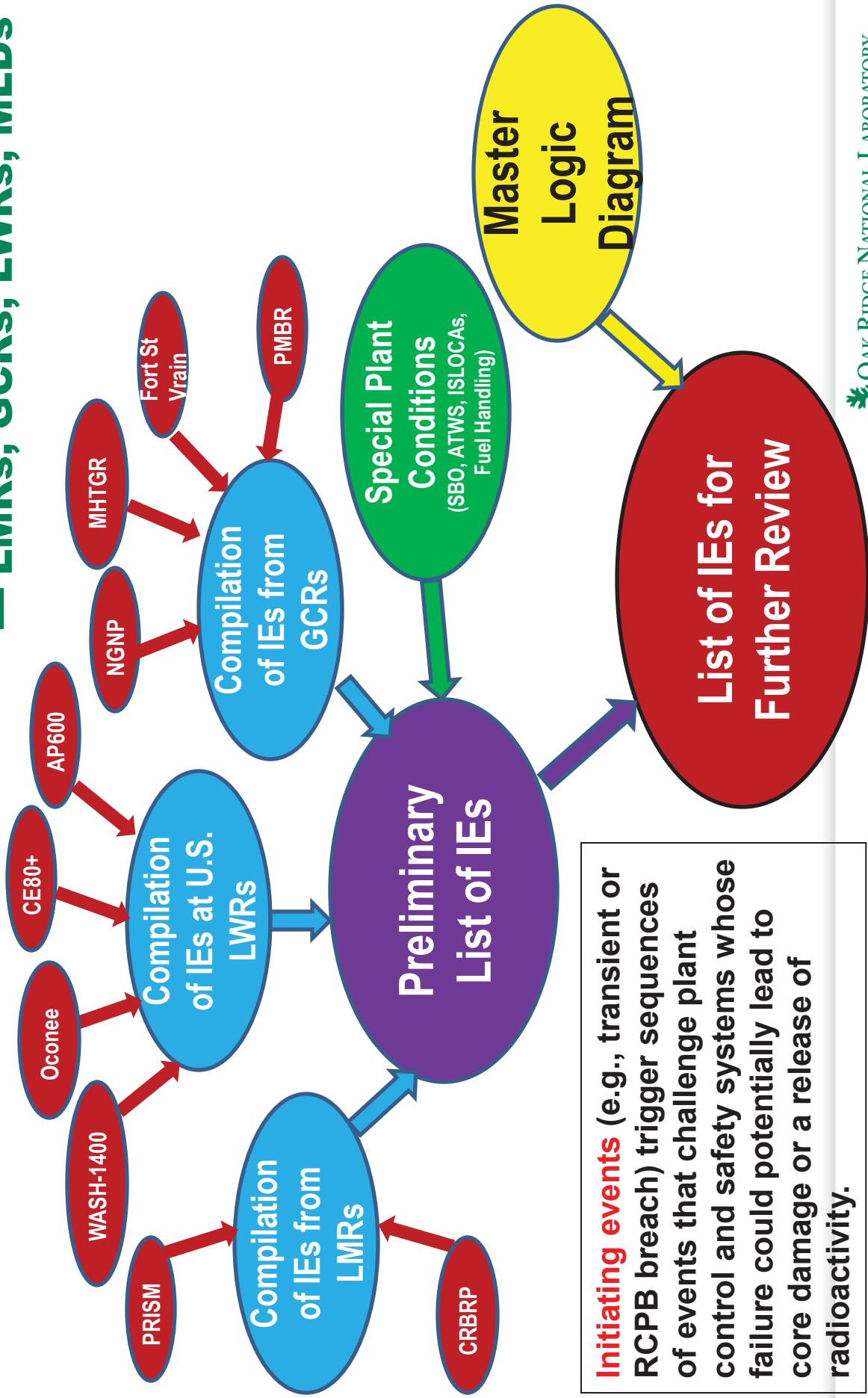
To Ensure Completeness, a Systematic Review Process was Used to Identify Potential IEs

- Master Logic Diagram (MLD)
 - Used to guide the identification and grouping of IEs to ensure completeness
 - Follows a step-by-step process of defining the failure modes of each structure, system, and component and the impacts of these failures in challenging the barriers and safety functions
- Previous PRA studies and reviews
 - GCRs, LMRs, LWRs, WASH-1400
- Guidance from revision to ASME RA-S-2008 for non-LWRs (Draft)
 - Reactor-technology neutral basis
 - Different sources of radioactive material both within and outside the reactor core, different plant operating states (e.g., shutdown, low power), internal and external IEs
- DOE hazards assessments
 - DOE's hazards assessments focus on the sources and release of radioactive material

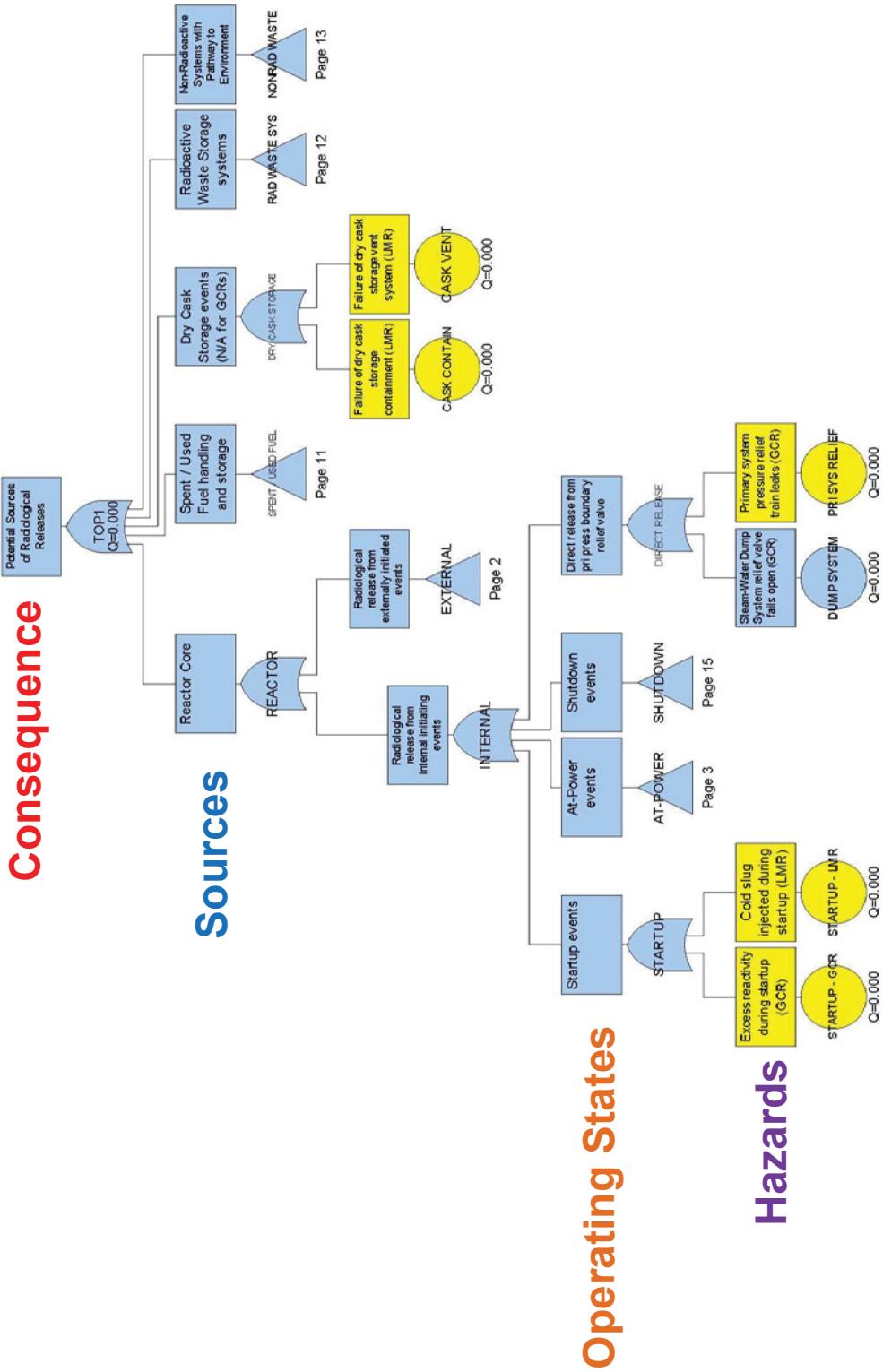
Components of the Systematic Process Blanket All Sources, Operating States, and Hazards



The Process for Developing the List of IEs Used Information from Multiple Sources – LMRs, GCRs, LWRs, MLDs



MLD Addresses All Sources, Operating States, and Potential Hazards that Challenge Site



The Systematic Review Identified Several IEs to Supplement Previous Lists

- **IEs from reviews for U.S. PWRs**

- Interfacing System Loss-of-Coolant Accident (ISLOCA) (GCR)
- Multiple and single steam generator tube ruptures
- Support system failures (e.g., ac power, dc power, offsite power, cooling systems)
- Turbine trip

- **IEs from special events**

- Anticipated transients without scram (ATWS)
- Station blackout (SBO)
- Spent/used fuel cooling

- **IEs from master logic diagram**

- Startup events
- Shutdown events
- Dry cask storage events
- Radioactive waste system failures

Grouping of IEs

- Grouping of IEs reduces the number of IEs to be evaluated
- Grouping of IEs was based on similarity of response into a single, bounding, higher-level event
 - Master logic diagram inherently groups events because of its logical structure
 - Previous studies that grouped events provided insights into responses
- Grouping of IEs was within, not between, operating states
 - Some potential overlap of IEs (e.g., release from RCPB in at-power and refueling states)

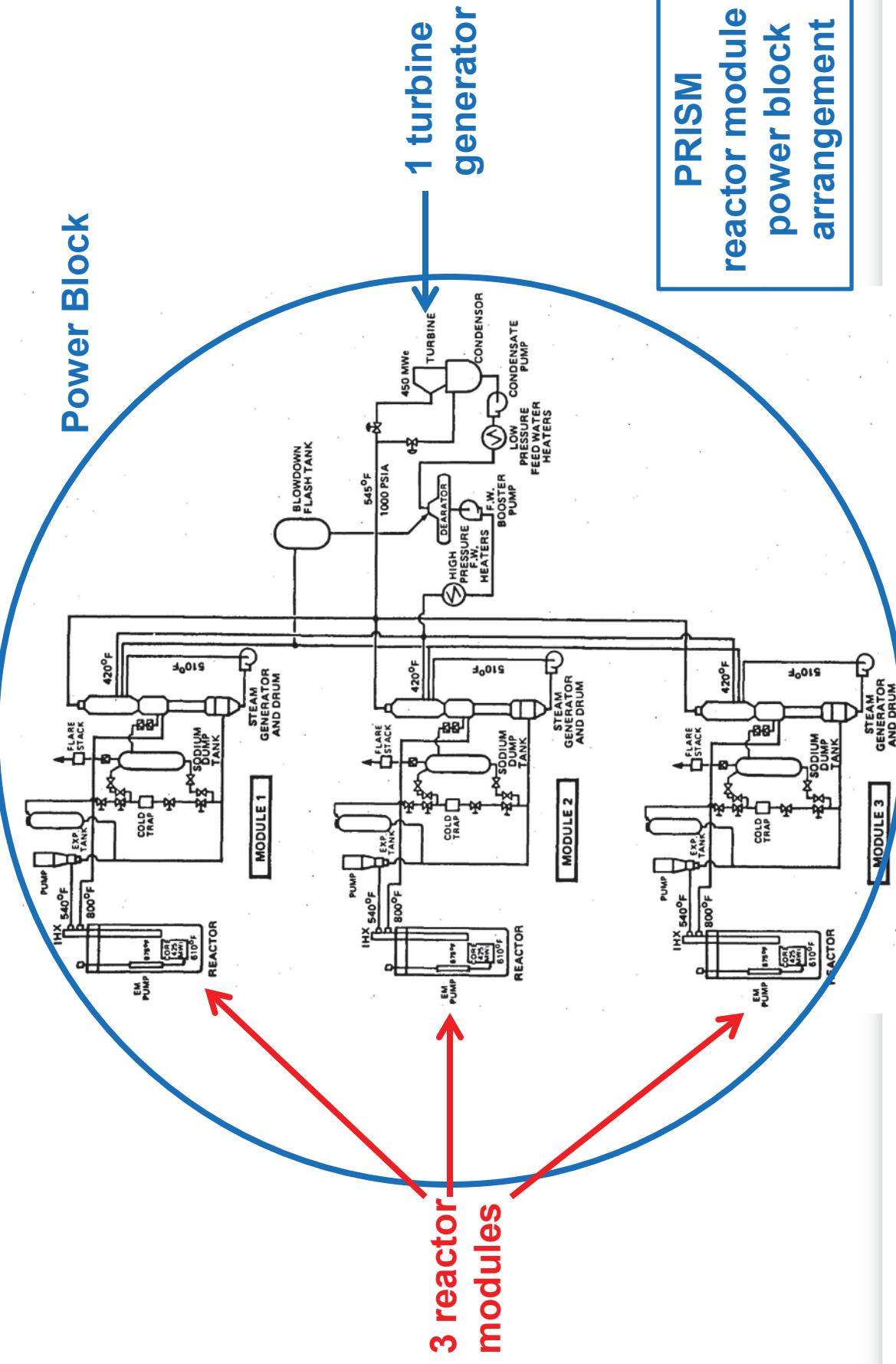
Grouping Results

- The potential IEs were grouped into 36 IEs selected for further review
 - PRISM identified 21 IEs for further review; MHTGR identified 8

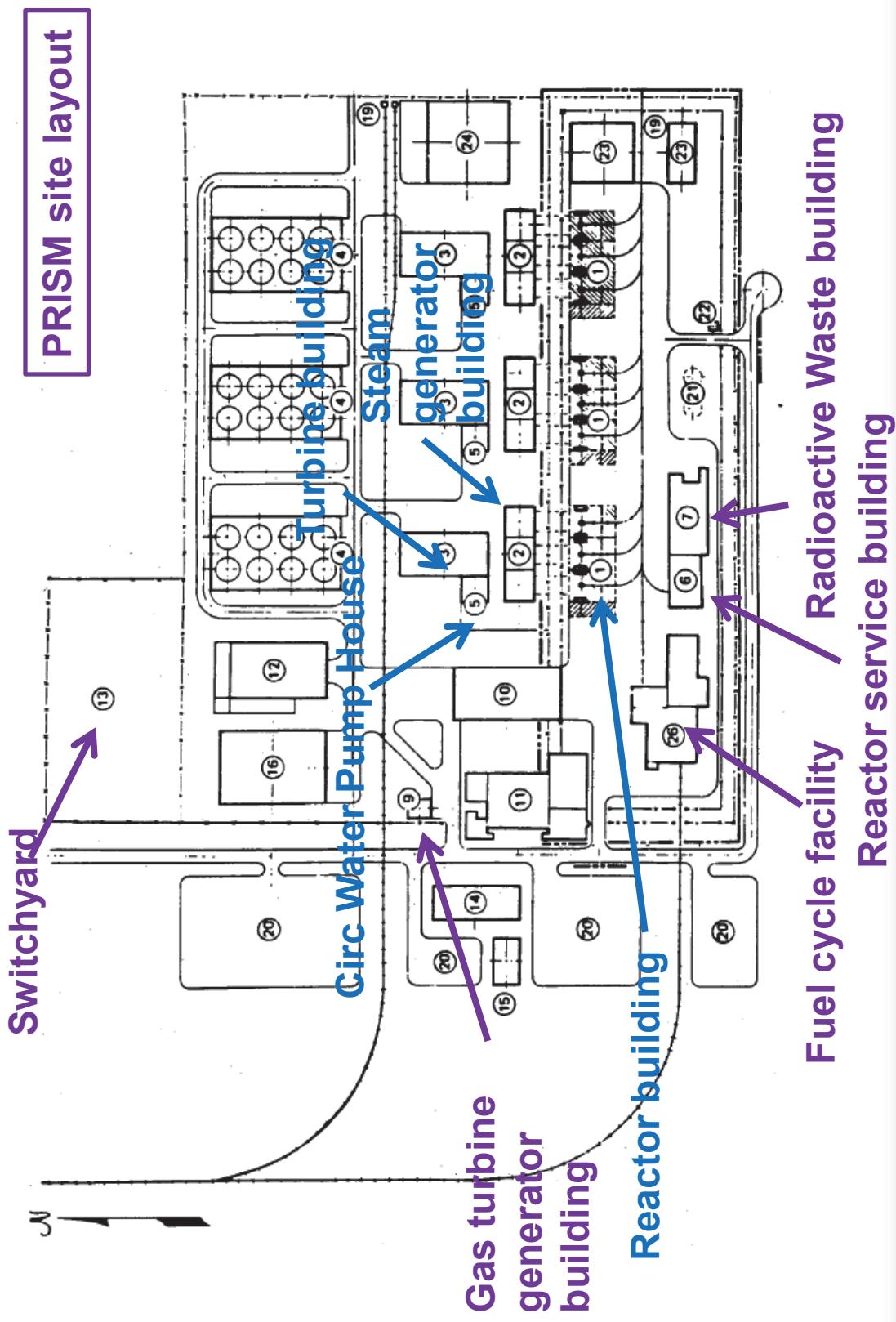
IE Group	aSMR	PRISM	MHTGR
Transients	8	9	5
RCPB / ICPB breaches	5	4	1
Chemical reactions (GCR)	0		
IS-LOCA (GCR)	1		
Special initiators (support system failures)	6	2	1
Structural faults	0		
Internal flooding or fire events	2		
External hazards	2	3	1
Direct releases (GCR)	1		
Startup / low power operations	2		
Shutdown and refueling	2	3	
Spent / used fuel handling and storage	2		
Dry cask storage (LMR)	2		
Radioactive waste systems	3		
Nonradioactive waste systems	0		
			8
			21
			36

At Power IEs

Special Issue—Integrated Site Risk Systems are Shared Among Reactor Modules



Special Issue—Integrated Site Risk Systems are Shared Among Power Blocks at a Site



A Multi-Unit PRA Is Needed to Understand the Integrated Risk

- Current PRAs are usually performed for a single unit.
- Because aSMRs may operate as multiple modular units with a centralized control room and increased dependencies from shared systems, a single-unit PRA may not adequately measure the risks or properly identify dependencies among units.
- The CDF for the multi-unit PRA for the Brown Ferry Nuclear Plant was **4 times greater** than that for Unit 2 alone.
- Because of the increased level of direct and indirect interactions among units, it is apparent that the PRAs for modular reactor designs need to specifically address potential interactions among the multiple units.

The Multiple Module Design of aSMRs Increases the Likelihood of Initiators at a Single Module Affecting Multiple Modules

- Examples of systems that are typically shared between independent units at a plant site include electric power, control and service air, HVAC, radwaste, service water, raw cooling water, fire protection, plant communication systems, etc.
- Examples of increased dependencies at modular plants include operational dependencies and sharing of staff
 - An ATWS in 1 module requires a trip of 1 or more other modules (MHTGR)
 - Failure of the service water system results in a loss of Helium Transport System (HTS) cooling to all 4 modules (MHTGR)
 - Loss of non-class IE ac power results in the loss of HTS cooling (MHTGR)
 - The design philosophy of the PRISM is to form a single power plant station *with respect to power generation and control* (PRISM)

Conclusions and Insights

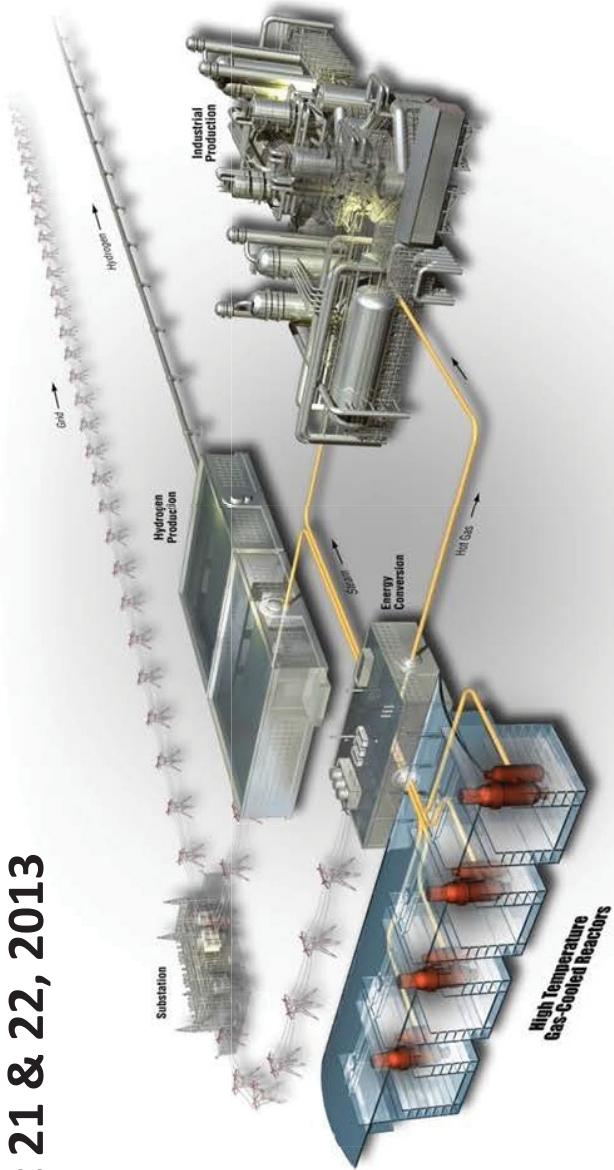
- The preliminary list of IEs, which were identified following current standard PRA procedures, yielded a conservative set of IEs for further review, grouping, and development of accident sequences
 - Number of events—The review selected 36 generic IEs for review compared with 21 for PRISM and 8 for the MIHTGR. Differences are primarily from the limited scope of previous studies, which did not include dry cask storage, refueling, startup, waste storage, etc.
 - Grouping—Some of the newly identified generic IEs may be determined to be subsets of each other. For example, a general transient accident sequence includes ATWS; both are currently identified as separate transients.
 - Accident sequences—Developing the accident sequences may result in further grouping of events. For example, an RCPB breach during refueling has a smaller consequence than an RCPB breach during power operations but probably has a higher frequency of occurrence.
- Understanding the integrated site risk associated with multiple modular units with a centralized control room and shared systems is necessary to understanding plant strengths and weaknesses.



NGNP Licensing Overview

AdvSMR PRA Technical Exchange Meeting

August 21 & 22, 2013



www.inl.gov



NRC-DOE Licensing Strategy (Report to Congress - 2008)

“It will be necessary to resolve the following NRC licensing technical, policy, and programmatic issues and obtain Commission decisions on these matters”

- Acceptable basis for event-specific mechanistic source term calculation, including the siting source term
- Approach for using frequency and consequence to select licensing-basis events
- Allowable dose consequences for the licensing-basis event categories
- Requirements and criteria for functional performance of the NGNP containment as a radiological barrier



Probabilistic Event Selection – SECY-03-0047

- In SECY-03-0047, the NRC staff proposed a probabilistic approach for identifying events to be considered in a plant's design basis provided:
 - Plant and fuel performance are sufficiently understood, and
 - Deterministic engineering judgment is used to bound analysis uncertainties
- Recommendations to Commission:
 - Modify Commission guidance to put greater emphasis on use of risk information by allowing use of probabilistic event selection approach
 - Allow a probabilistic approach for the safety classification of structures, systems, and components (SSCs)
 - Replace single failure criterion with a probabilistic (reliability) criterion
- Places greater emphasis on PRA quality, completeness, and documentation

Licensing Basis Event (LBE) Selection

- Licensing Basis Events determine when Top Level Regulatory Criteria (TLRC) must be met
- Selected throughout design and licensing process with risk insights from comprehensive full scope PRA that addresses uncertainties
 - Start with deterministic events based on history of related design/licensing efforts; used for scoping studies and early design development
 - As design matures, PRA risk-informs the event selection
- Includes anticipated events (AEs), design basis events (DBEs), beyond design basis events (BDBEs), and design basis accidents (DBAs)
- Comprehensive: Addresses a full-spectrum of internal and external events on a per plant-year basis, including event sequences that could affect multiple reactor modules

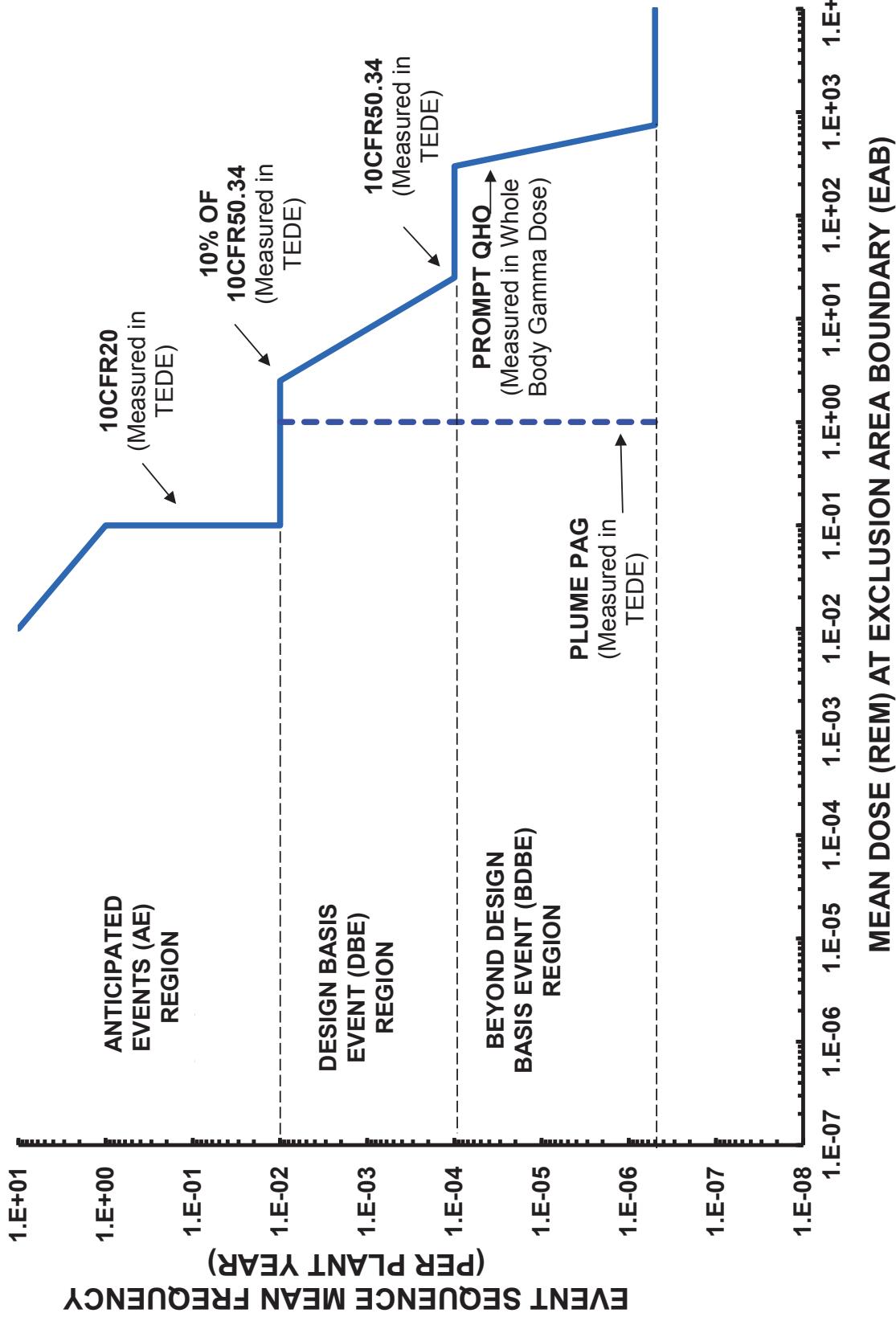
Top Level Regulatory Criteria (TLRC)

- Anticipated Events (AEs) – 10 CFR 20
 - 100 mrem - cumulative annual dose to an individual at the Exclusion Area Boundary (EAB)
 - Realistically calculated
- Design Basis Events (DBEs) – 10 CFR 50.34
 - 25 rem TEDE – event based; dose to an individual at EAB
 - Conservatively calculated
- Beyond Design Basis Events (BDBEs)
 - Based on cumulative public dose limits derived from the quantitative health objectives (QHOs)
 - Realistically calculated

Design Basis Accident Derivation

- DBAs (analyzed in Chapter 15 of SARS) are deterministically derived from DBEs (developed from the PRA) by assuming that only safety-related structures, systems, and components (SSCs) are available
- The event sequence frequency for some DBAs is expected to fall in or below the BDBE region as a result of the assumed failure of the non-safety related SSCs
- Consistent with regulatory practice, DBAs must meet the DBE dose limits based on conservative (upper 95%) analyses

NGNP Frequency-Consequence Curve



Advancement of Risk-Informed, Performance-Based (RIPB) Event Selection Approach

- Proposed approach to placing TLRC on a frequency-consequence (F-C) curve
 - Logical basis for demonstrating that the design meets applicable regulatory criteria for public health and safety
- Event category names (i.e., AE, DBE, BDBE) and descriptions
- Frequency and consequence uncertainty analysis
- Per-plant-year approach for addressing the integrated risk in PRA modeling for a plant with multiple reactor modules
- Event Category Frequency Ranges
 - AE Lower Frequency Cutoff: 10^{-2}
 - DBE Range: 10^{-2} to 10^{-4}
 - BDBE Range: 10^{-4} to 5×10^{-7}
- Use of risk information for SSC safety classification

Reducing Regulatory Uncertainty for Modular HTGR Deployment

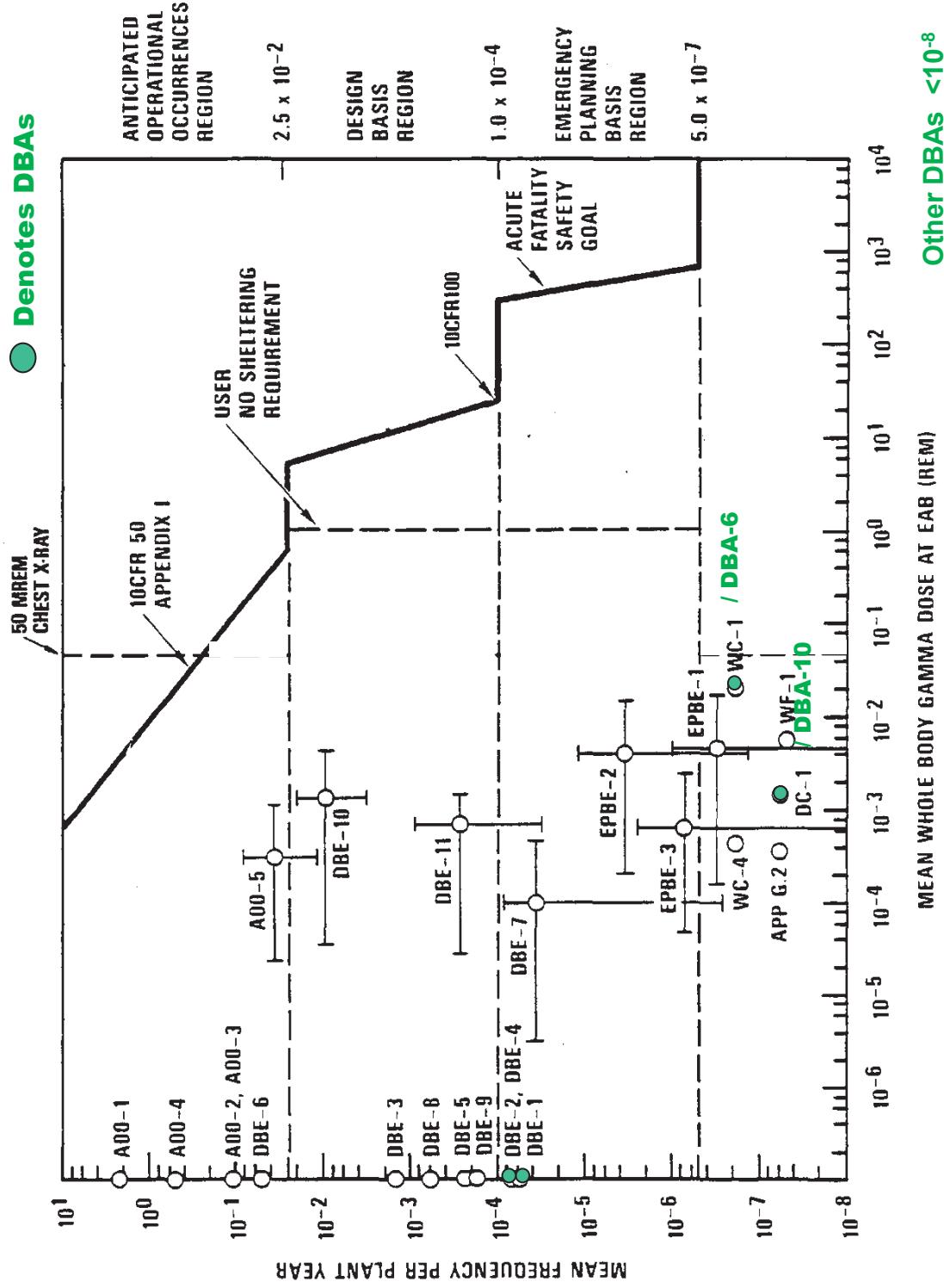
- DOE is focused on the resolution of long-standing HTGR licensability issues, and eliminating the significant uncertainty that goes with them
- Status of key issue resolution generally well understood, with significant progress from DOE-NRC pre-licensing interactions
- However, significant uncertainty remains regarding the process for design basis accident (DBA) selection
 - Deterministic event selection: no apparent lower limit on event sequence frequency
 - Potentially hampers the ability of the designer and applicant to demonstrate that safety margins are increased, as directed by the Commission's Advanced Reactor Policy Statement
 - Creates significant uncertainty for NGNP stakeholders and other advanced reactor designs
 - NRC is concerned with reliability/quality of PRA for selecting events
- RIPPB approach could be affected by NRC activities related to NUREG-2150, NUREG-1860, and Near-Term Task Force Recommendation 1 (Fukushima)

Impact of PRA on Future Licensing

- The PRA will be used by advanced plants to establish the set of event sequences to be considered in licensing the plant
- This contrasts with the deterministic methods used to establish events for the current operating fleet and recently licensed reactors
- New application of PRA will result in:
 - Establishment of requirements and guidance for technical adequacy of the plant PRA
 - These requirements are likely to be different and more demanding than the current requirements for the existing fleet; increased emphasis on risk requires a corresponding enhancement in PRA quality
- Application of deterministic judgment:
 - Modeling uncertainties
 - Completeness uncertainties
 - Lack of adequate or directly applicable data

Backup Slides

MHTGR DBEs, DBAs, and BDBEs on F-C Plot (circa 1987)



Safety Approach and Design Basis Summary

- Top objective is to meet the NRC offsite dose requirements and EPA Protective Action Guides (PAGs) at the Exclusion Area Boundary (EAB) for spectrum of events within and beyond the design basis
- Responsive to Advanced Reactor Policy
- Modular HTGR designs employ multiple concentric, independent barriers to meet radionuclide retention requirements – these barriers comprise the Functional Containment
 - Fuel Elements
 - Fuel kernels
 - Particle coatings (most important barrier)
 - Compact matrix and fuel element graphite
 - Helium Pressure Boundary
 - Reactor Building
- Emphasis is on radionuclide retention at the source within the TRISO fuel coatings

Siting Source Term Summary

- The NGNP approach to SSTs is essentially the same as that proposed by DOE in the MHTGR PSID and accepted by the NRC staff in NUREG-1338
- The approach is consistent with discussions of containment function and mechanistic source terms in more recent NRC SECY documents and with approaches previously reviewed by the NRC staff for modular HTGRs
- The approach implements a modular HTGR-appropriate interpretation of the 10CFR50.34 (10CFR52.79) footnote regarding siting evaluation
- Limiting DBAs are evaluated to determine SSTs
- Further, to ensure that there are no cliff edge effects, physically plausible Bounding Event Sequences (with frequencies below the BDBE region), including those involving graphite oxidation, are deterministically chosen and considered

Fuel Qualification and Radionuclide Retention Summary

- Fuel Development and Qualification Program is providing data, under an NRC-accepted QA program, necessary to better understand fuel performance and fission product behavior for modular HTGRs
- Fuel program is laying the technical foundation needed to qualify UCO TRISO fuel made to fabrication process and product specifications within an envelope of operating and accident conditions that are expected to be bounding for modular HTGRs
- Results to date are consistent with current design assumptions about fuel performance and radionuclide retention. The program is obtaining additional data to support model development and validation
- Results to date support the safety design basis, including the functional containment and mechanistic source term approaches
- It is expected that operation of the first modular HTGR will confirm the design assumptions

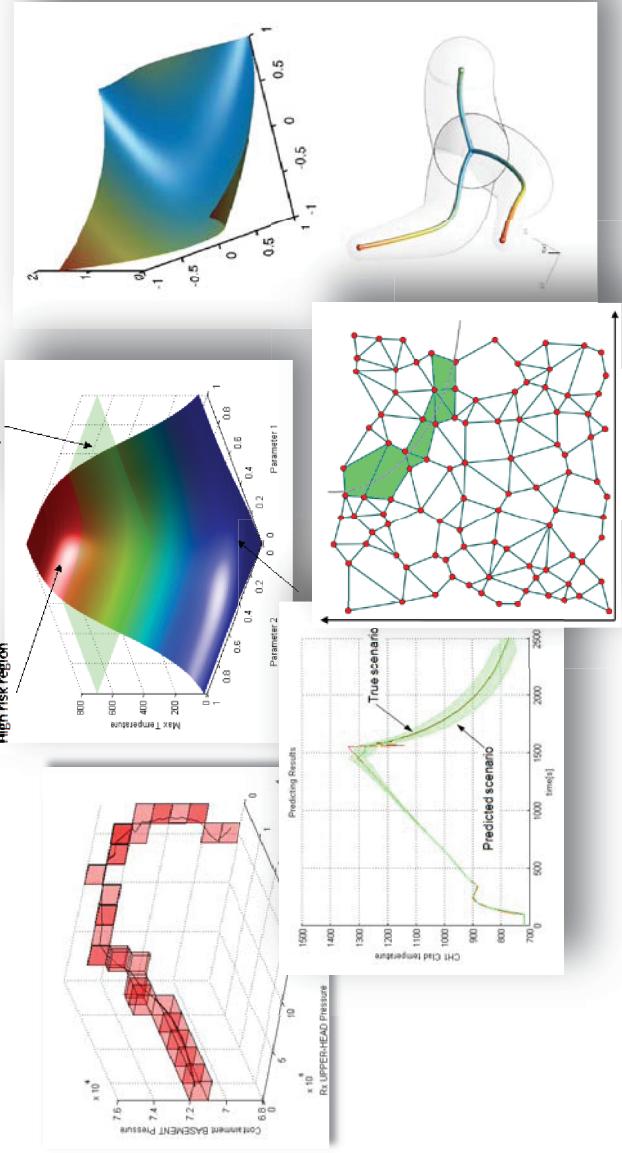
Functional Containment Performance Summary

- Radionuclide retention within fuel during normal operation with relatively low inventory released to helium pressure boundary (HPB)
- Limiting LBEs characterized by:
 - An initial release from the HPB depending on leak/break/pressure relief size
 - A larger, delayed release from the fuel
 - Functional Containment will meet 10CFR50.34 (10 CFR 52.79) at the EAB with margin, without consideration of radionuclide retention by the reactor building, for the wide spectrum of DBEs and DBAs
 - Functional Containment will meet the NGNP design target EPA PAGs at the EAB with margin, with consideration of radionuclide retention by the reactor building, for the wide spectrum of DBEs, DBAs, and DBDEs

Simulation Based PRA: Methods and Algorithms to Generate, Analyze, and Visualize Data

Diego Mandelli, Curtis Smith

August 22nd, 2013



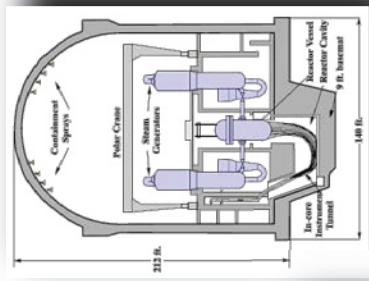
www.inl.gov



Simulation Based PRA: Outline

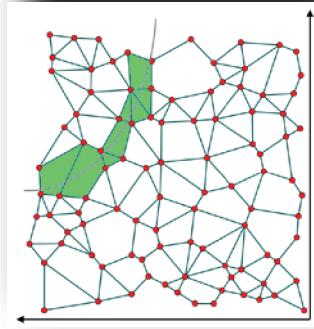
Three Major Parts/Steps:

1. Modeling (RELAP, MELCOR, MAACS)



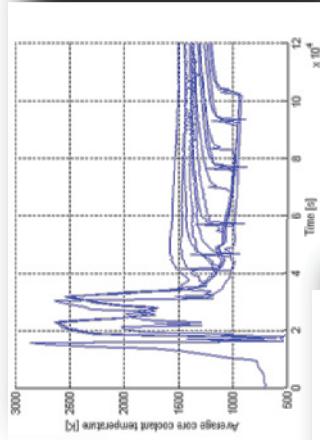
1. Generate data

- Adaptive sampling
- Reduced order models
- System emulators



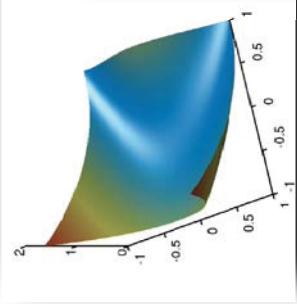
1. Analyze time dependent data

- Clustering
- Symbolic conversion



2. Visualize data

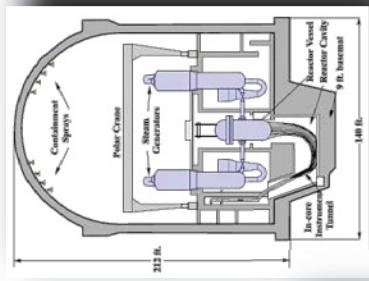
- Topology based



Simulation Based PRA: Outline

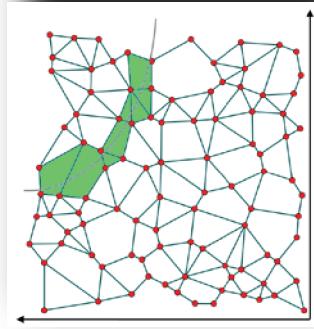
Three Major Parts/Steps:

1. Modeling (RELAP, MELCOR, MAACS)



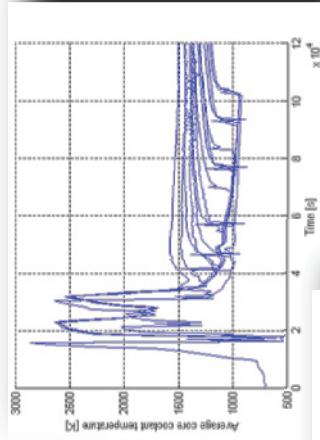
1. Generate data

- Adaptive sampling
- Reduced order models
- System emulators



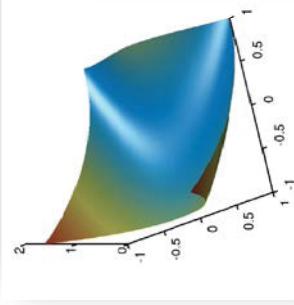
1. Analyze time dependent data

- Clustering
- Symbolic conversion



2. Visualize data

- Topology based



Data Generation

- PRA applications
 - Determine: $p_{failure} = \int_{\Omega} p df_1(\omega) \cdot p df_2(\omega) d\omega$

- Strategies:

1. Calculate the integral directly

- Monte-Carlo (MC):
 - 1. Sample timing of events
 - 2. Run a single simulation
 - 3. Repeat 1. and 2. N times

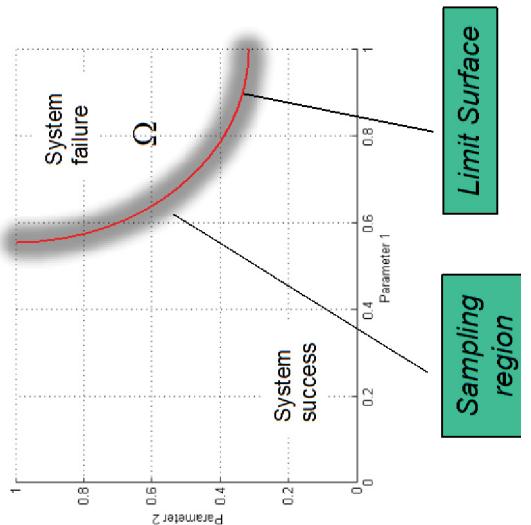
- Dynamic Event Trees (DETs):
 - Branch Scheduler
 - System Simulator

Branching occurs when particular conditions have been reached

- Value of specific variables
 - Specific time instants
 - Plant status

2. Evaluate only boundaries of Ω

- Estimate boundaries
- Concentrate samples around such boundaries



Data Generation

For large systems, several **problems** arise if MC or DET are used:

- The set of uncertain parameters is very large
- The computational costs are very high
- Many regions of the input space are not of interest

The space of the possible solutions can be sampled only very sparsely

This precludes the ability to fully analyze the impact of uncertainties on the system dynamics

Understanding of a system depends heavily on where we query

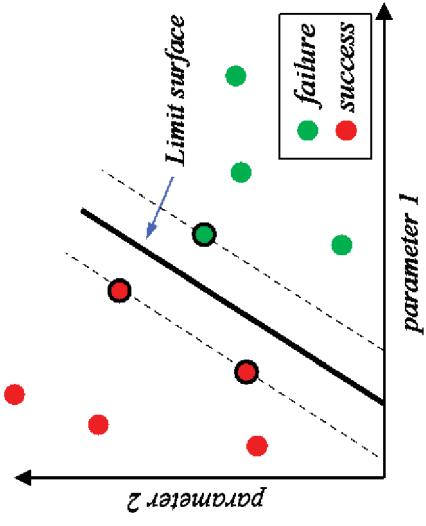
The scope of adaptive sampling is to identify the:

- Set of relevant parameters
- Regions that are of interest for the user

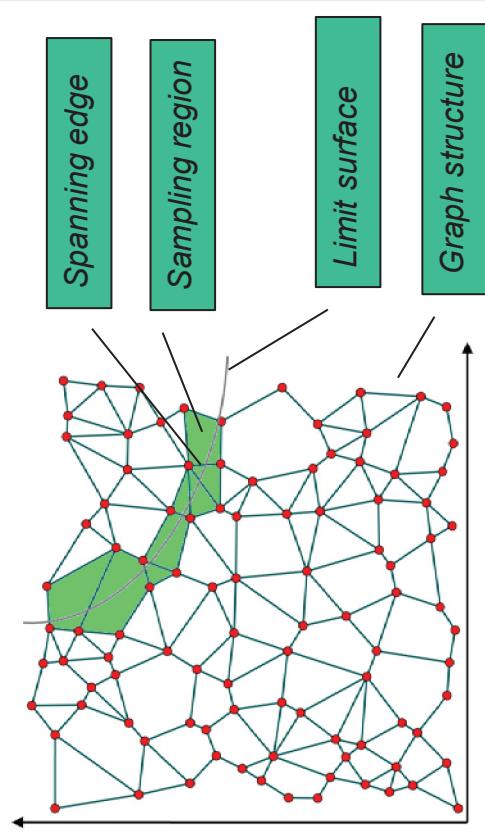
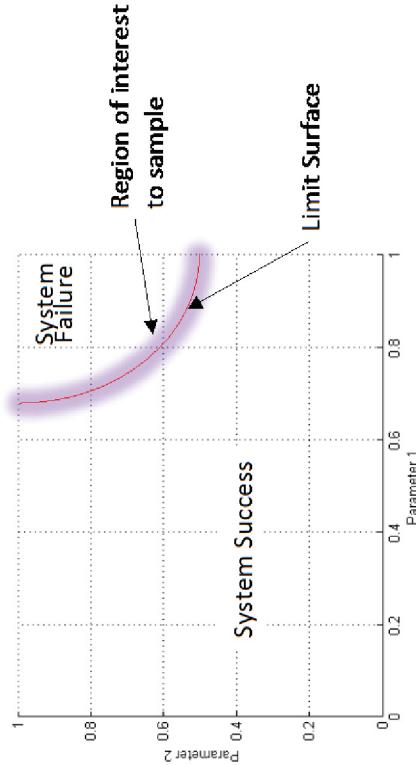
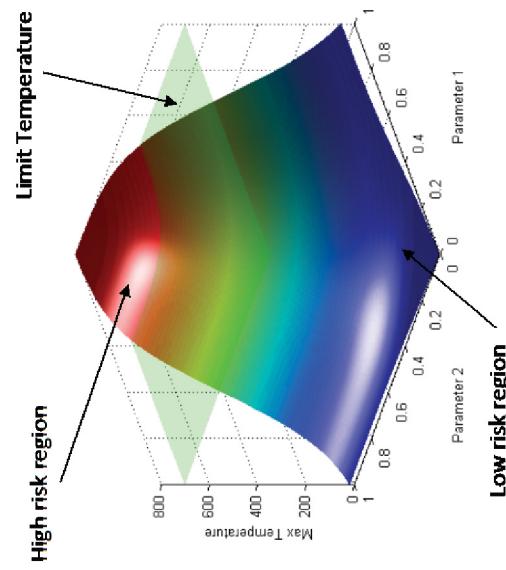
Performed by iteratively guiding the choice of the next sample by analyzing the previous sampling history

Adaptive Sampling

1- Data Driven: Geometric determination of the limit surface

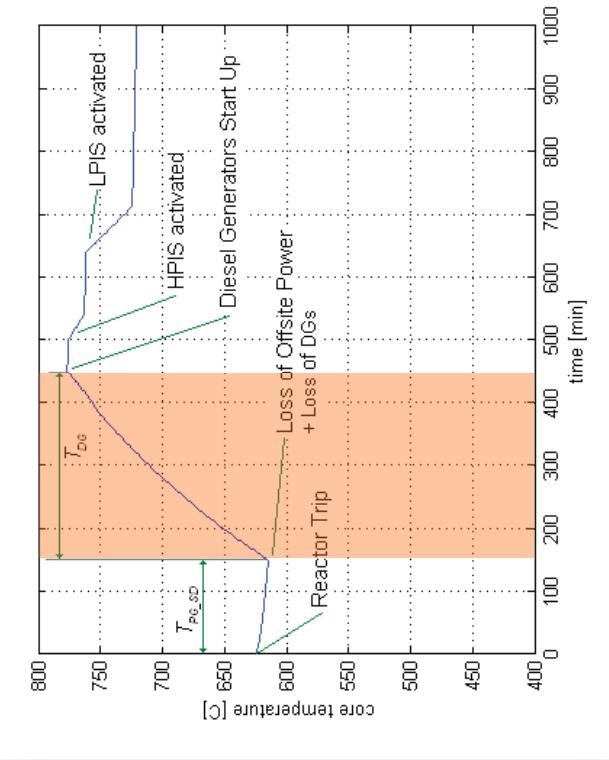


2- Model Driven: Prediction of system outcome (e.g., T_{MAX}): surrogate model



Example of Application: PWR SBO

Analyze uncertainties associated with the time at which the offsite power is lost and the time associated with the diesel generators' recovery time

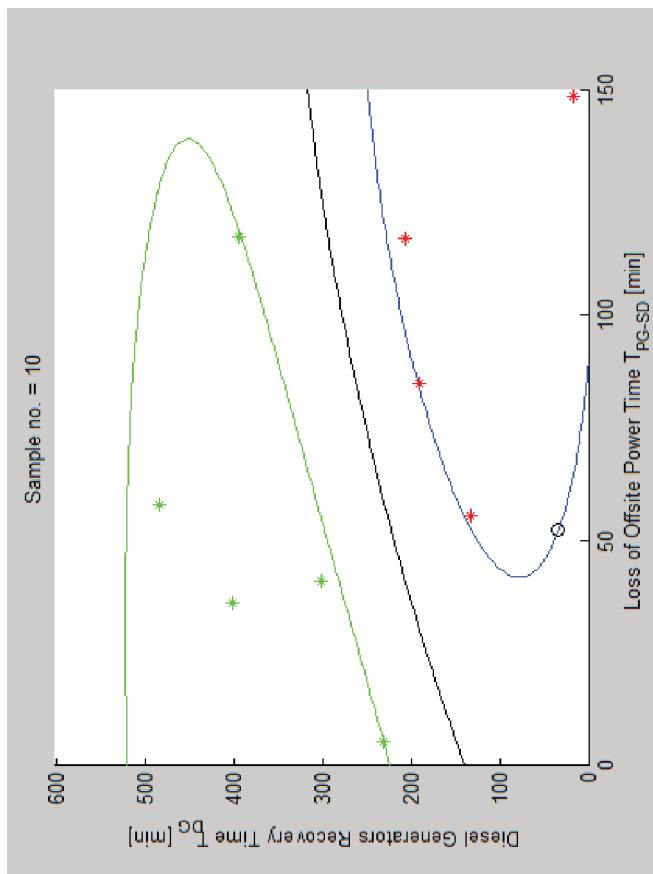


A typical scenario:

- External events force the reactor trip at $t = 0$
- Loss of Offsite Power at T_{PG_SD}
- Diesel generators fail to start.
- Temperature of the core starts to rise since heat removal is incapacitated. A failure condition is reached when temperature reaches 800°C.
- Diesel generators become available T_{DG} after LOOP condition and the ECCS is now able to remove decay heat.

Limit Surface

2-dimensional Issue Space: T_{PG_SD} vs. T_{DG}



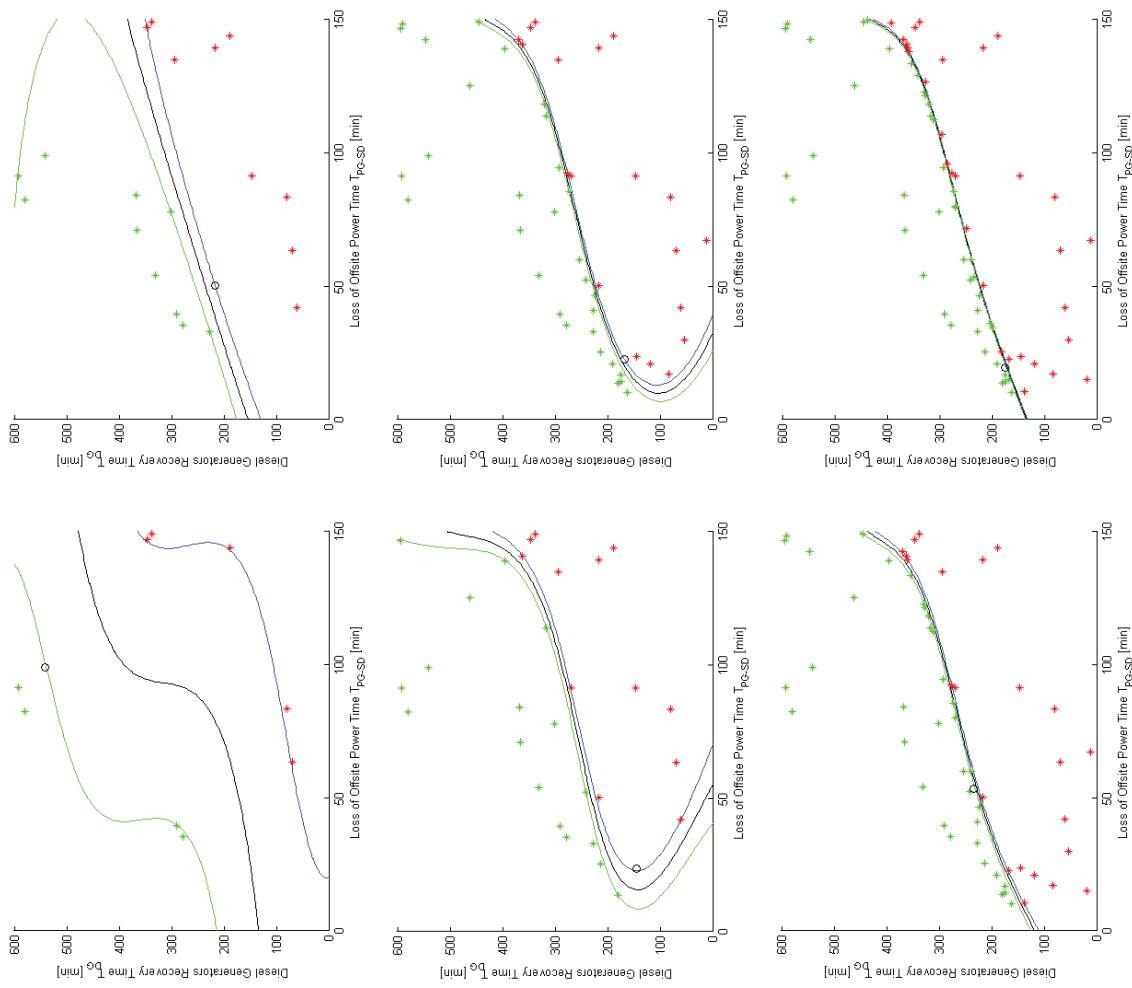
* = system success
 * = system failure
 ○ = next chosen sample

— = limit surface
 — = lower bound
 — = upper bound

Limit surface can be used to perform:

- Accurate estimation of failure probability (limit surface is distribution independent)
- Sensitivity analysis on the parameters (tangent along the limit surface)

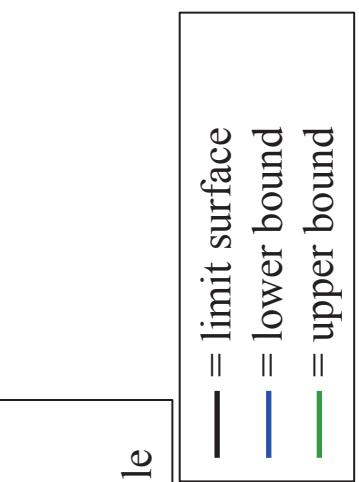
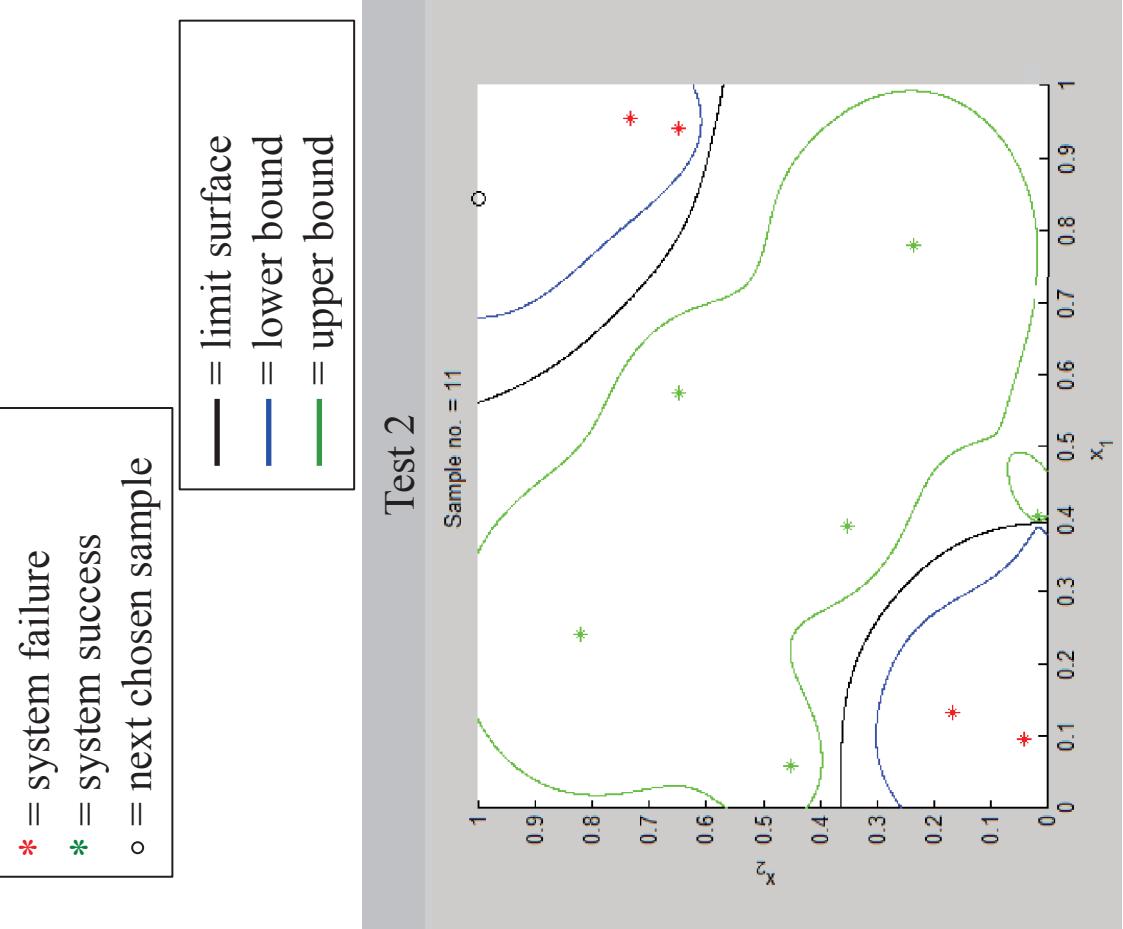
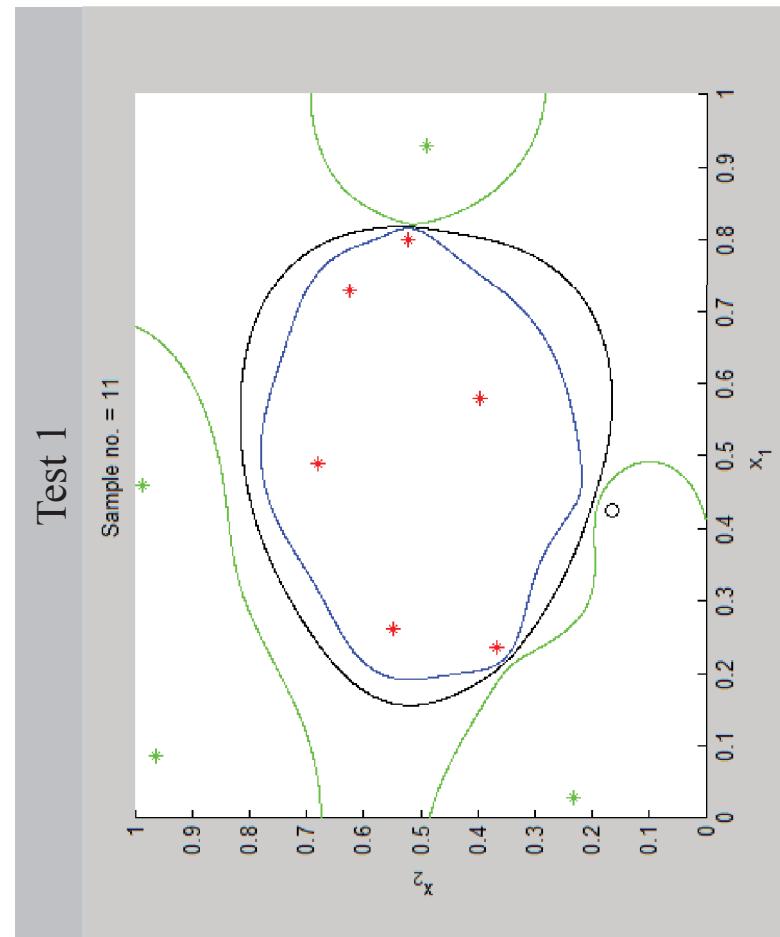
Limit Surface (in case the movie does *not* work)



* = system success
+ = system failure
○ = next chosen sample

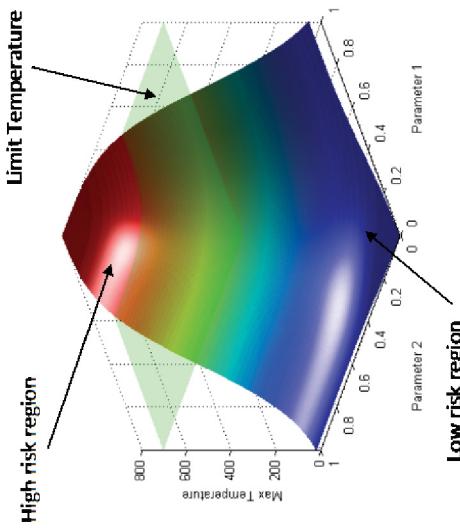
— = limit surface
— = lower bound
— = upper bound

Analytical Tests



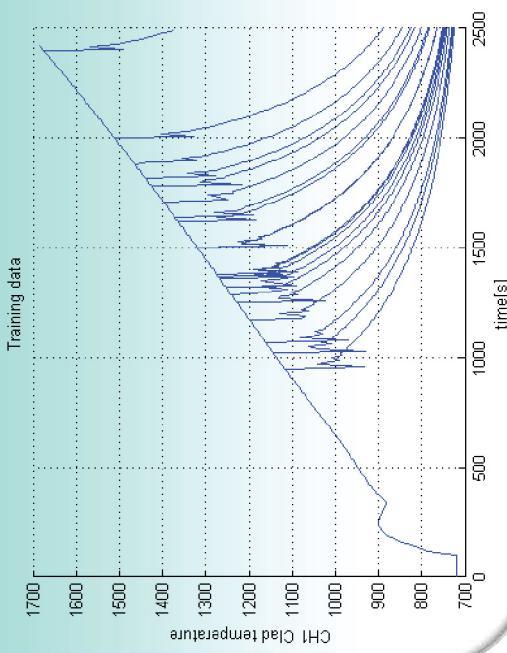
Expanding Model Driven Methodologies

- When the surrogate model is built, it is possible to predict **instantaneously** the system outcome without the need to run a simulation run
 - Microsecond vs. hours (or days)

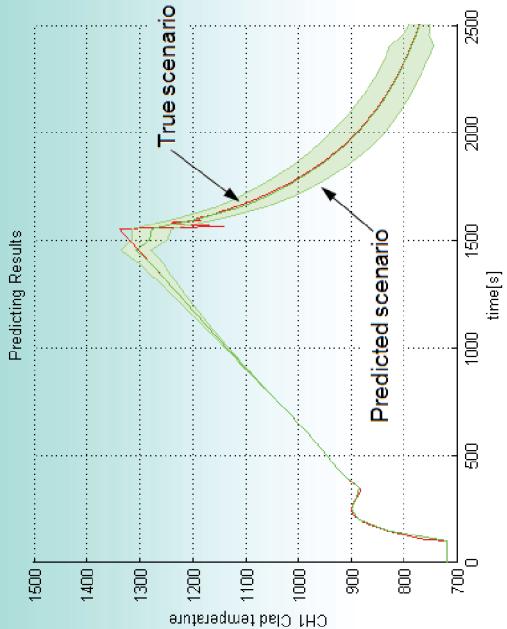


- Expand such algorithms to predict the full time history:
“**temporal predictor**”

Series of simulation runs performed by changing a single parameter p



Predicted scenario and true simulation run



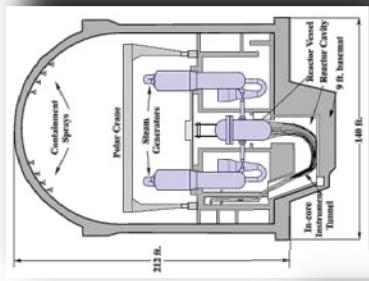
Learn for the set of simulation runs to predict temporal behavior for a new value of p



Simulation Based PRA: Outline

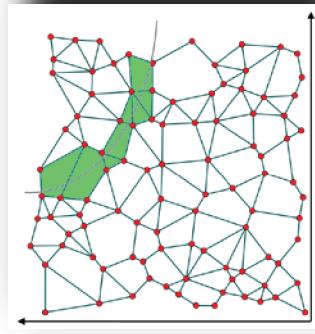
Three Major Parts/Steps:

1. Modeling (RELAP, MELCOR, MAACS)



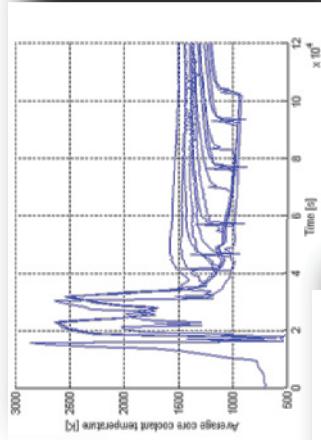
1. Generate data

- Adaptive sampling
- Reduced order models
- System emulators



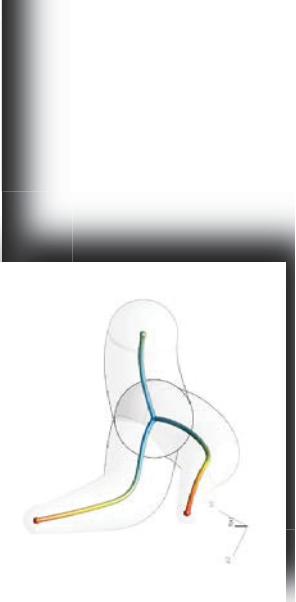
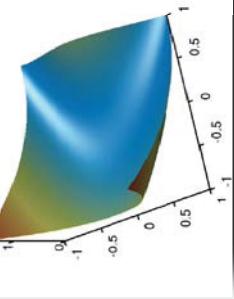
1. Analyze time dependent data

- Clustering
- Symbolic conversion



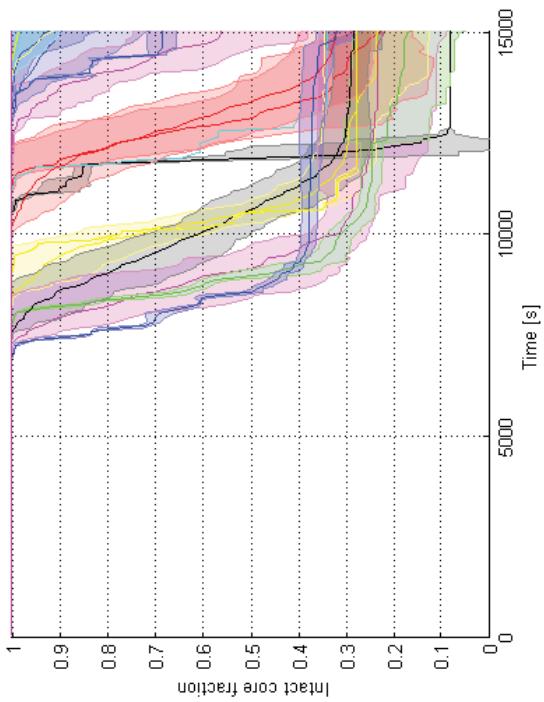
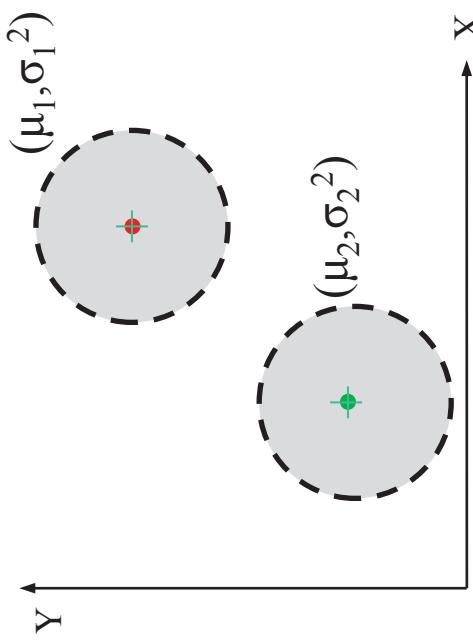
2. Visualize data

- Topology based



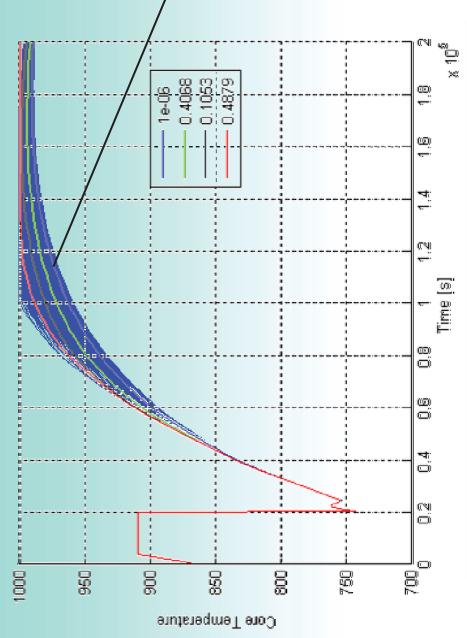
Clustering Time Dependent Data

- Scope: Analyze patterns
- Type of data: thousands of time dependent transients
- Consider the complete time history and not only the end result
- Approach: cluster data into groups
 - Define metric
 - Input clustering level
- Algorithms:
 - Data-centric: K-Means
 - Model-Centric: Density gradient based (Mean-Shift)

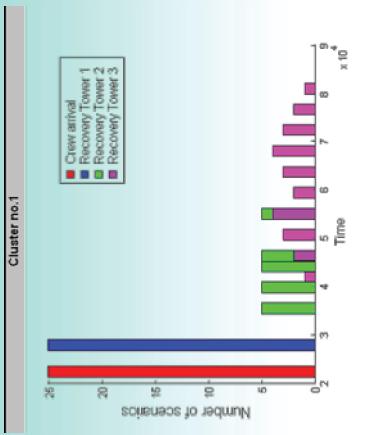


Data Analysis Applied to PRA

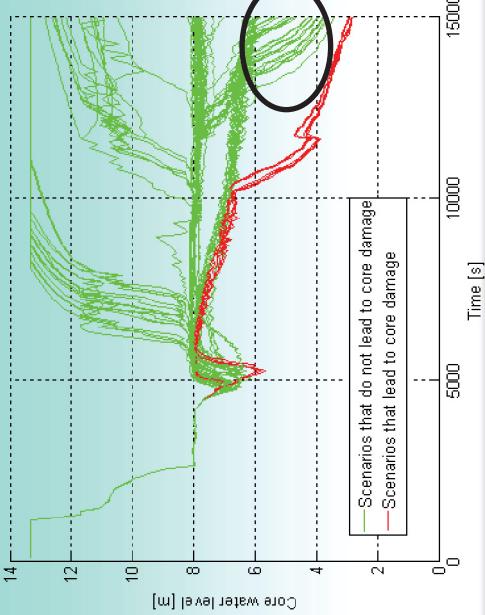
Identify correlations
between system dynamics
and timing of events



Identify distribution of events
for each cluster of scenarios



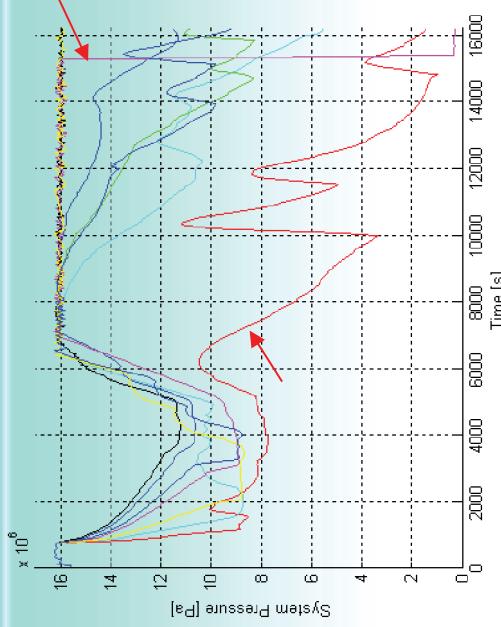
Evaluate “Near Misses” or scenarios that did
not lead to CD because mission time ended
before reaching CD



Identify clusters containing scenarios that lead
to both system failure and system success

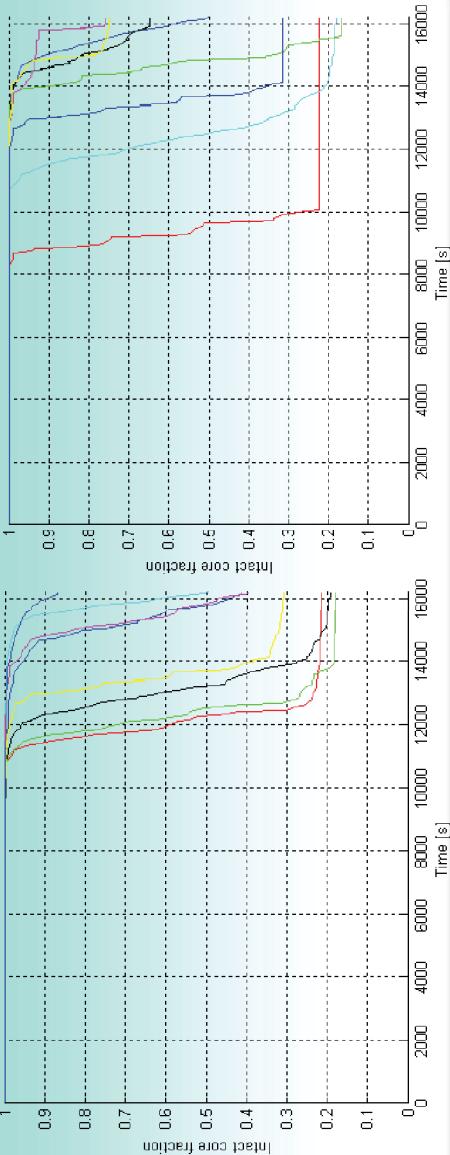
Data Analysis Applied to PRA

Identify outliers: “bogus” simulations whose dynamics are different from any other simulation (e.g., out of validity bounds for simulator parameters)



Evaluate system dynamics differences between different sets of analyses (System Design); e.g., different set of system recovery strategies

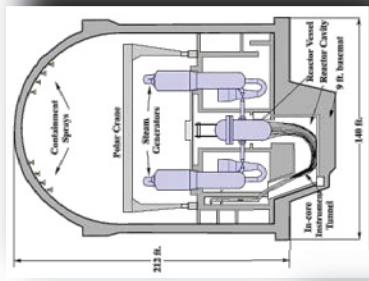
System Configuration 2



Simulation Based PRA: Outline

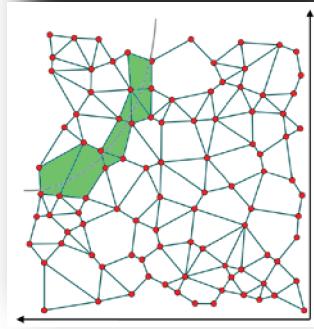
Three Major Parts/Steps:

1. Modeling (RELAP, MELCOR, MAACS)



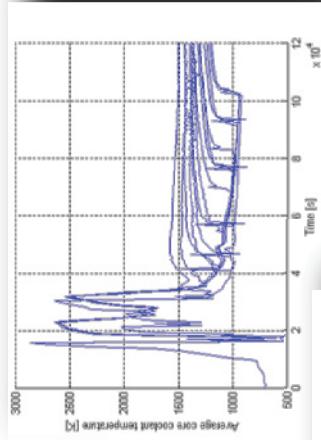
1. Generate data

- Adaptive sampling
- Reduced order models
- System emulators



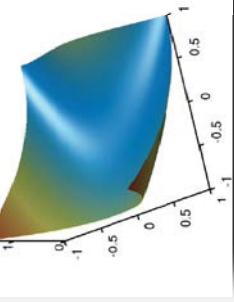
1. Analyze time dependent data

- Clustering
- Symbolic conversion



2. Visualize data

- Topology based



Data Visualization: HDViz

INL internally funded project with Scientific Computing and Imaging Institute (University of Utah)

Objective: Develop a software tool to **visualize high dimensional data** as:

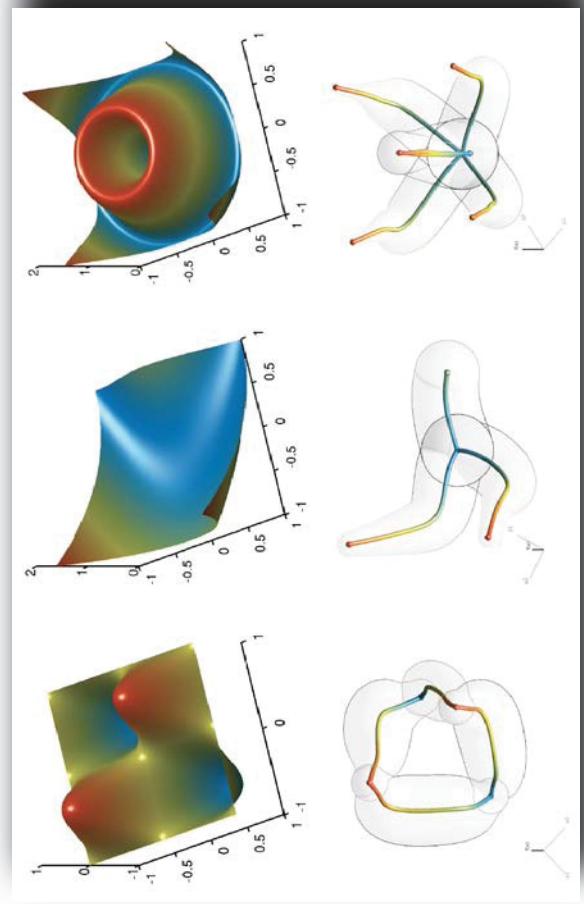
$$\text{system outcome} = f(\text{uncertain parameters})$$

Max clad temperature
Max containment pressure

Timing of events
HPI water flow rate
Initial power

Analysis:

- Exploiting the topological and geometric properties of the domain (Morse-Smale complex)
- Building statistical models based on its topological segmentations
- Providing interactive visual interfaces to facilitate such explorations.

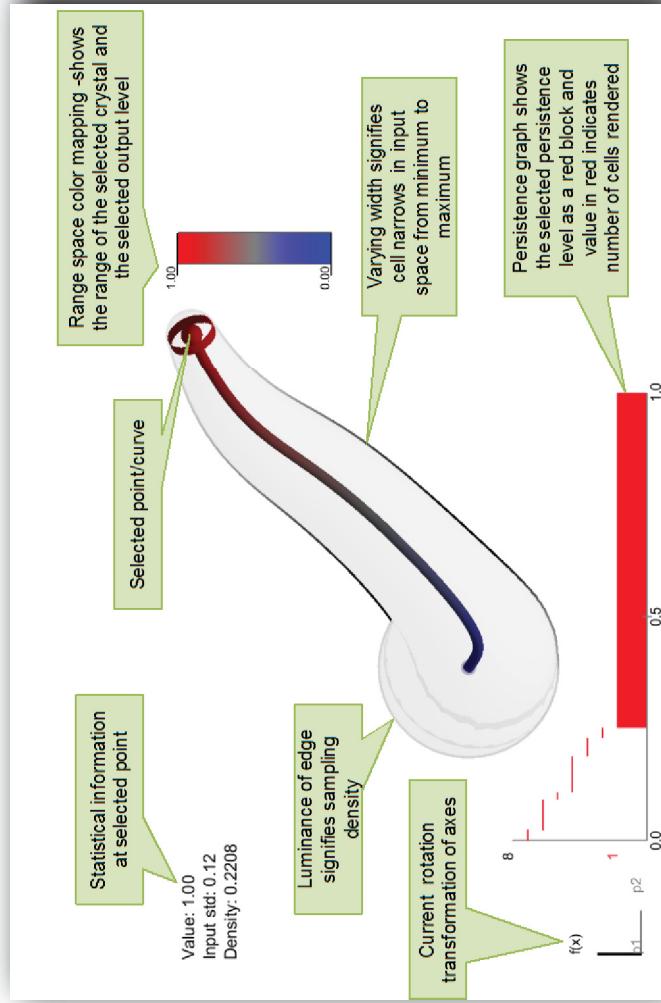
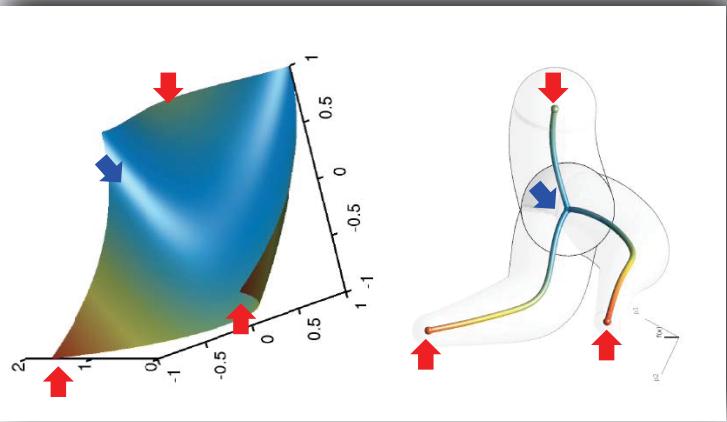


Data Visualization: HDViz

- Graphic overview of HDViz to visualize:

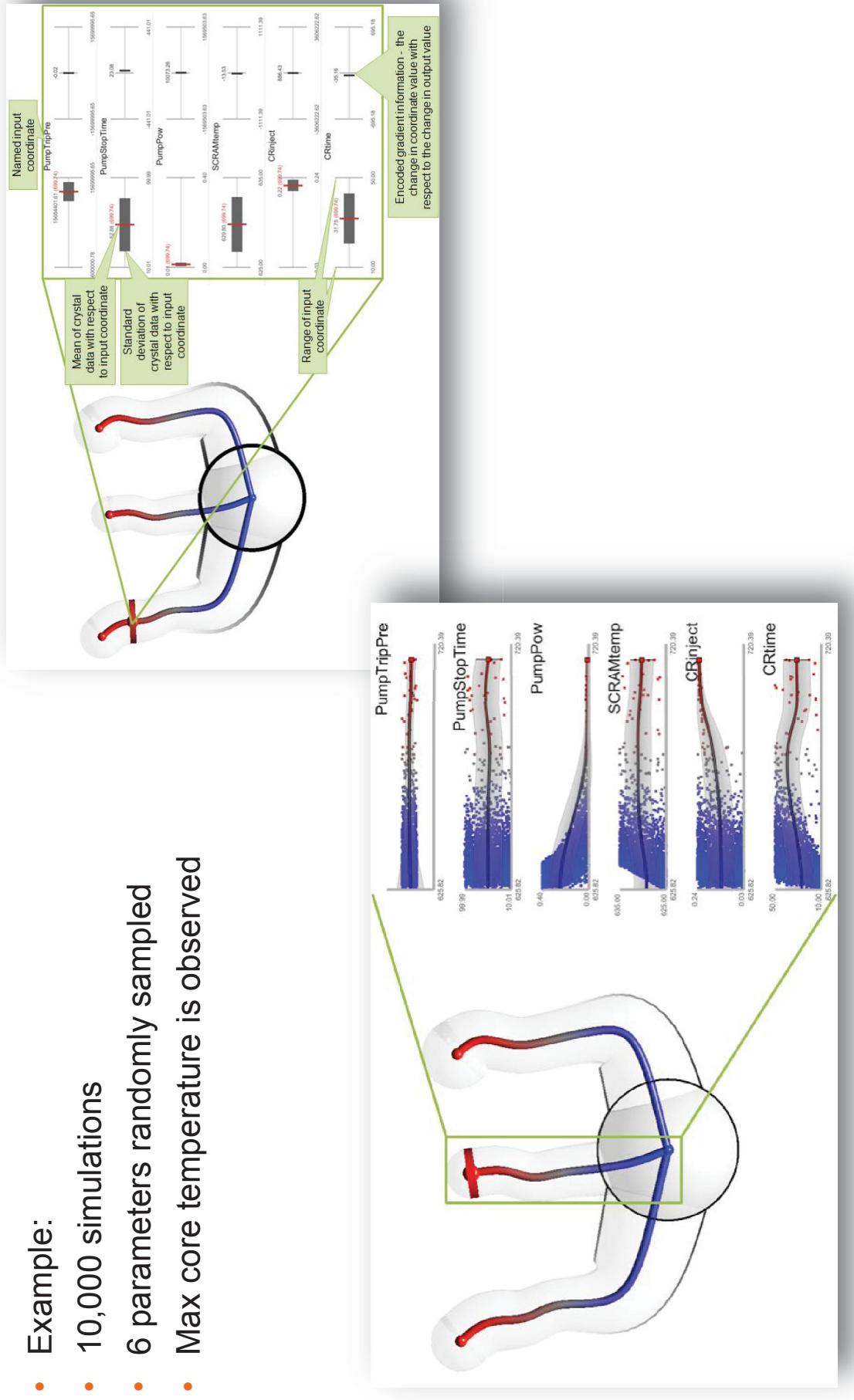
$$\text{system outcome} = f(\text{input parameters})$$

- Visualize the topological structure of f through the connection between its min(s) and max(es)



Data Visualization: HDViz

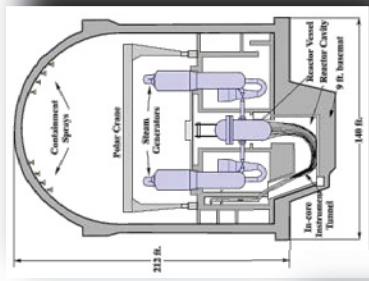
- Example:
- 10,000 simulations
- 6 parameters randomly sampled
- Max core temperature is observed



Simulation Based PRA: Outline

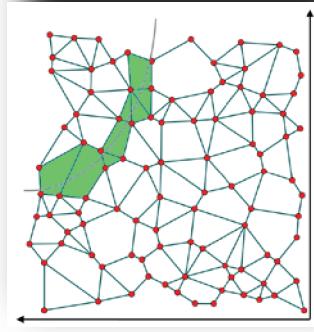
Three Major Parts/Steps:

1. Modeling (RELAP, MELCOR, MAACS)



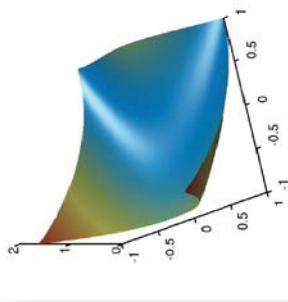
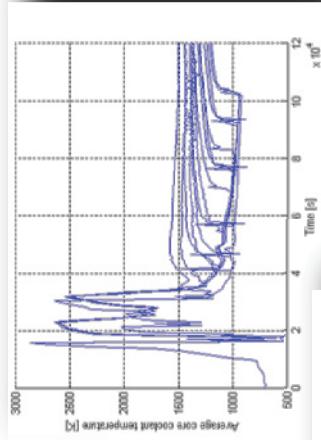
1. Generate data

- Adaptive sampling
- Reduced order models
- System emulators



1. Analyze time dependent data

- Clustering
- Symbolic conversion



2. Visualize data

- Topology based

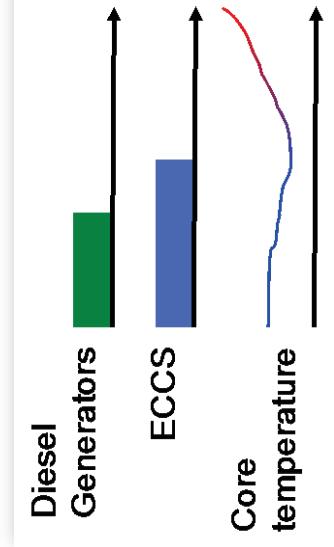


Symbolic Conversion

- Scope: identify local/global correlations between events and system dynamics

- Data:

- Continuous: state variables $\theta(t)$ (e.g., temperature)
- Discrete: time occurrence of events $(A_i, [t_{A_i,\alpha}, t_{A_i,\omega}])$



- Issue: Different data format

- Solution: Symbolic conversion

- Mining phrases need a specific grammar that for each event preserves:

- Duration
- Coincidence
- Order

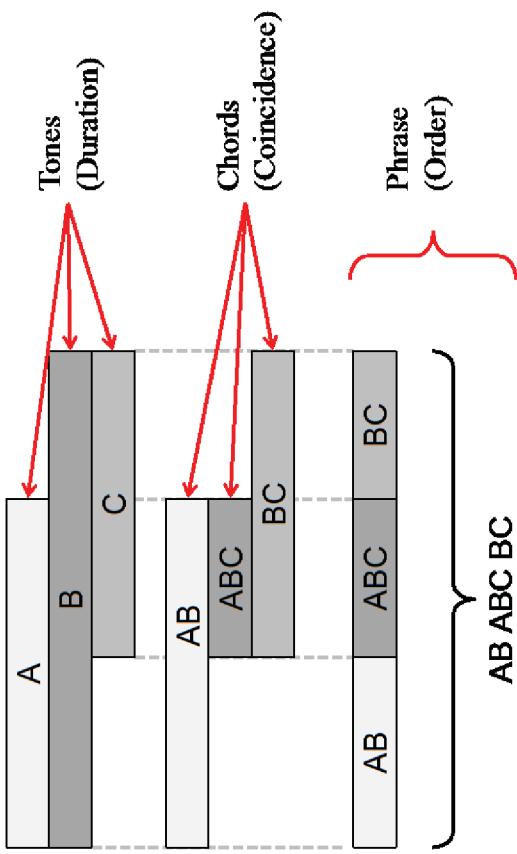
- Allen's interval 13 relations

	Freksa's semi-interval relations
before	older
meets	younger
overlaps	head to head
starts	A
during	B
finishes	B
equals	B

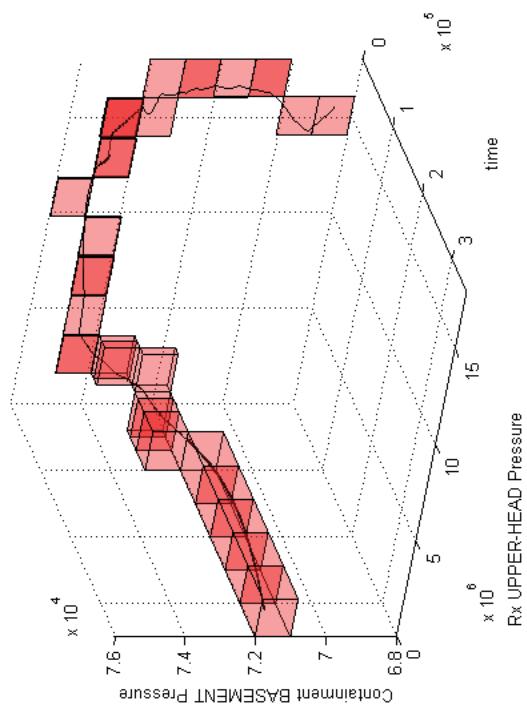
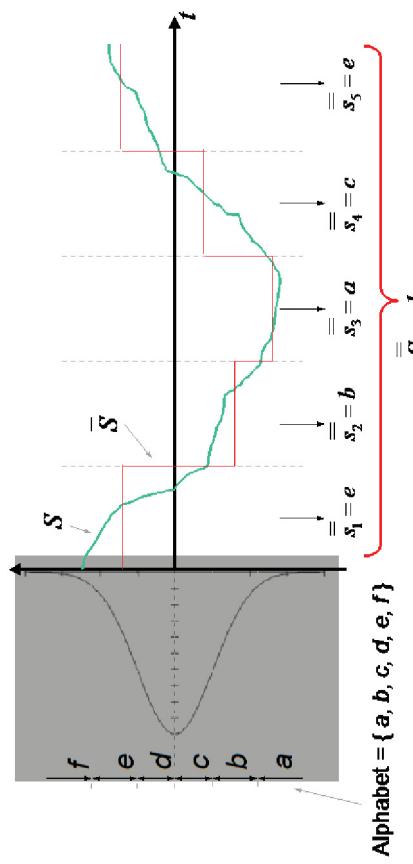
born before death	A
died after birth	B

Symbolic Conversion

1- Discrete Data: Time Series Knowledge Representation

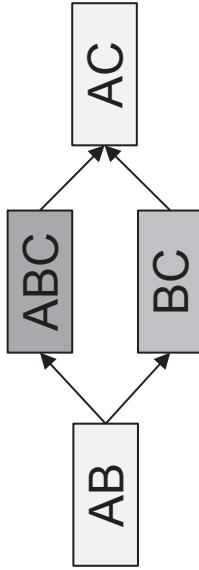


2- Continuous Data: Modified version of SAX



Symbolic Conversion

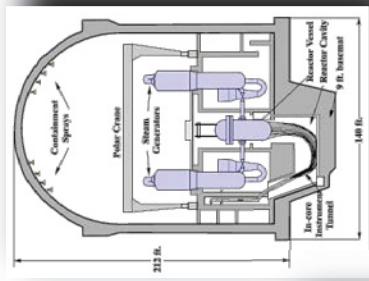
- Symbolic representation allows:
 - Whole time series clustering
 - Sub-series clustering
 - Motif discovery
 - Anomaly detection
- Available tools:
 - Markov Models
 - Decision Trees
 - Suffix Trees
 - Hashing
- Preliminary evaluation:
 - Great memory reduction
 - Computational reduction for clustering, search, and classification algorithms



Simulation Based PRA: Outline

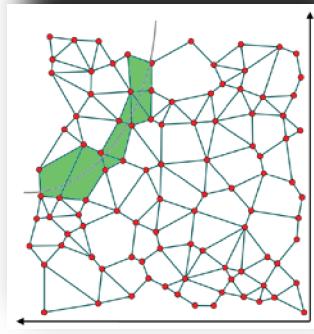
Three Major Parts/Steps:

1. Modeling (RELAP, MELCOR, MAACS)



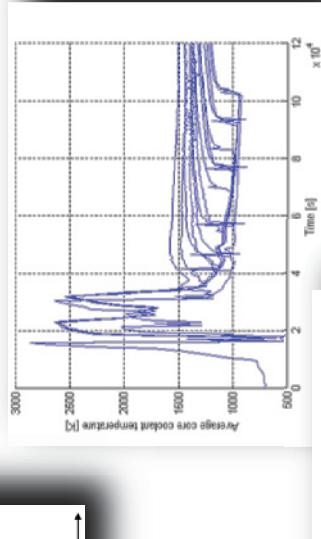
1. Generate data

- Adaptive sampling
- Reduced order models
- System emulators



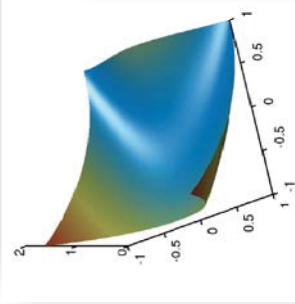
1. Analyze time dependent data

- Clustering
- Symbolic conversion



2. Visualize data

- Topology based





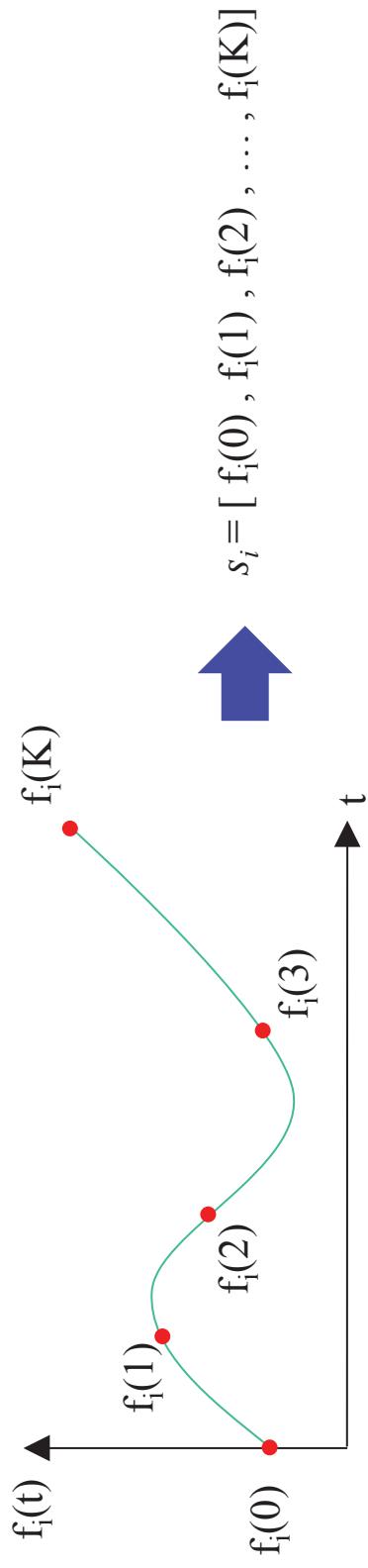
Backup Slides

Data Analysis Applied to PRA

How do we represent a single scenario s_i ? $\left\{ \begin{array}{l} \text{Multiple state variables } (\textcolor{red}{M} \text{ are chosen}) \\ \text{Time evolution} \end{array} \right.$



Multi-dimensional vector: Each component of this vector corresponds to the value of a variables sampled at a specific time instant



Dimensionality = (number of state variables) · (number of sampling instants) = $\textcolor{red}{M} \cdot \textcolor{red}{K}$

Sequence of letters (Symbolic Conversion): discretization of both state variables and temporal scales



Data Analysis Applied to PRA: Similarities Metrics

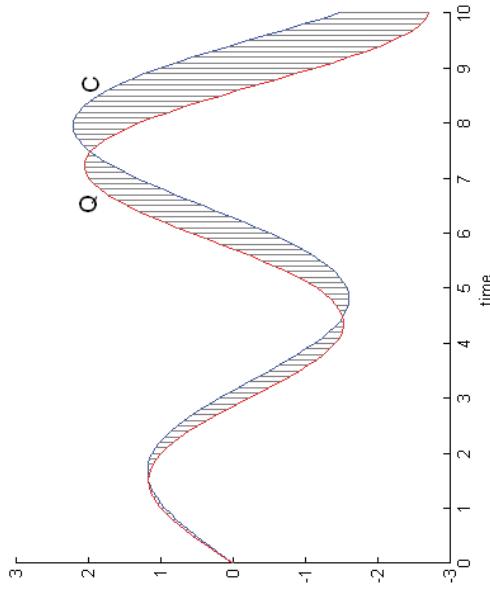
Given two time series :

$$Q = (q_1, q_2, \dots, q_n)$$

$$C = (c_1, c_2, \dots, c_n)$$

the Euclidean distance is given by:

$$d_2(Q, C) = \sqrt{\sum_{t=1}^n (q_t - c_t)^2}$$



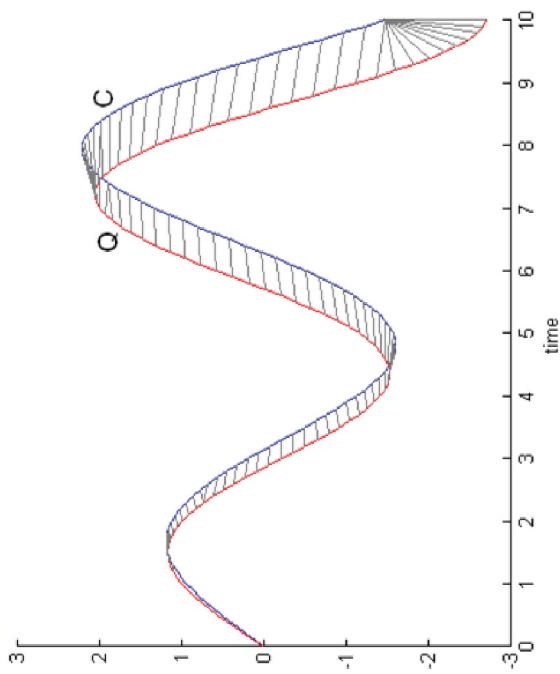
Disadvantages:

1. Requires time series of equal length
2. Weakness of sensitivity to distortion in time axis

Data Analysis Applied to PRA: Similarities Metrics

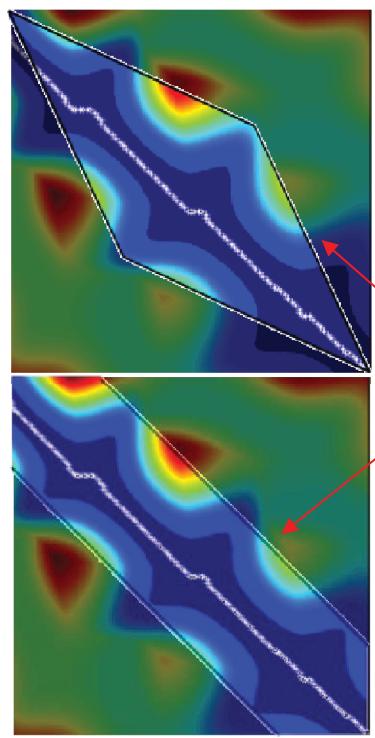
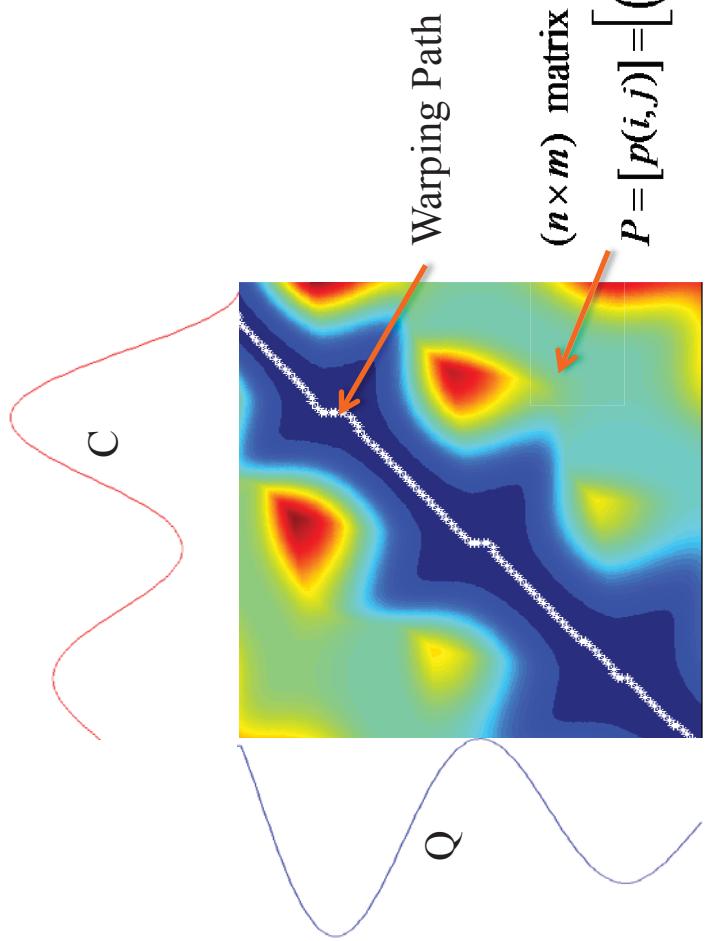
$$\begin{aligned} Q &= (q_1, q_2, \dots, q_n) \\ C &= (c_1, c_2, \dots, c_m) \end{aligned}$$

Given two time series :



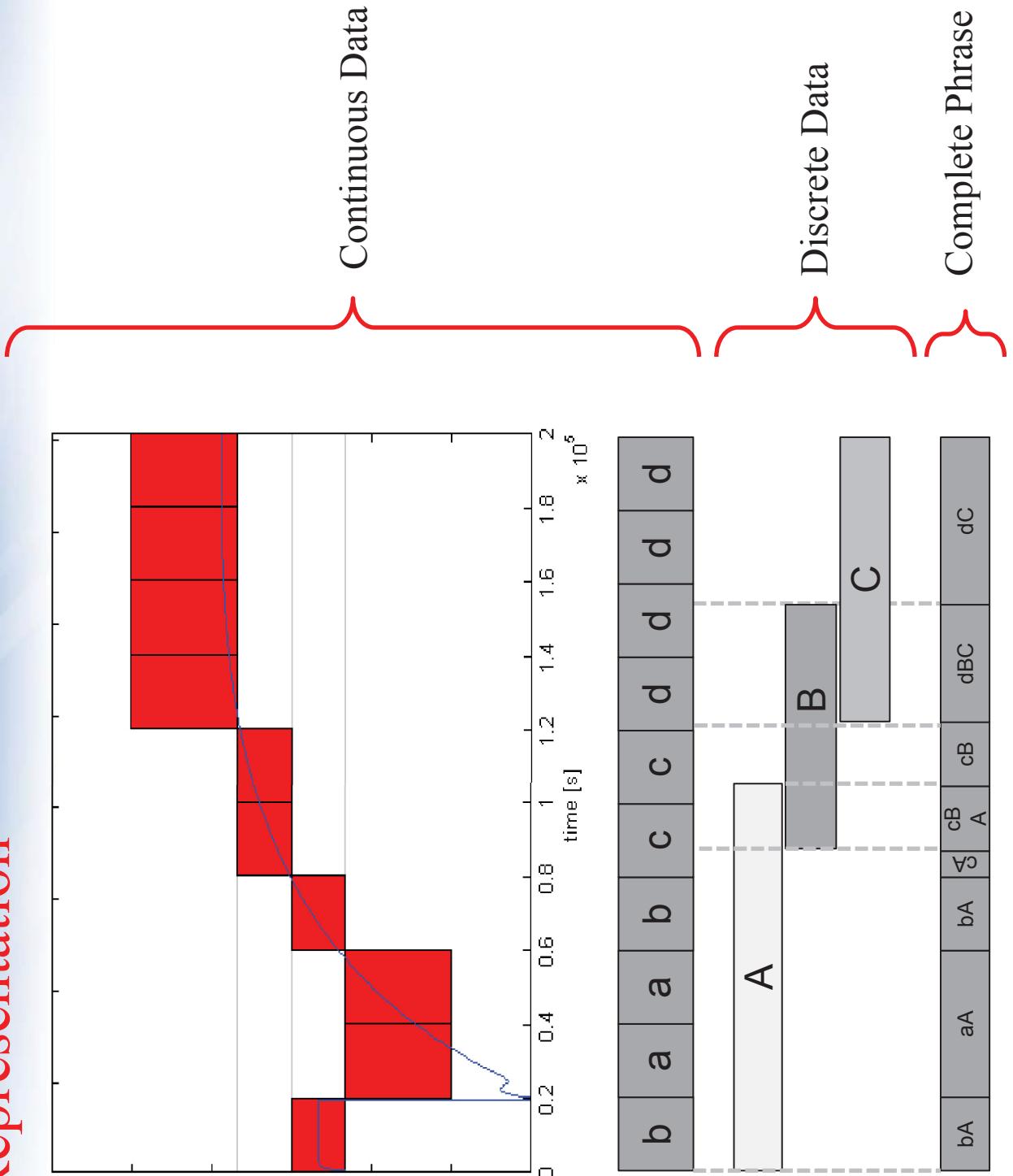
the Dynamic Time Warping distance is given by:

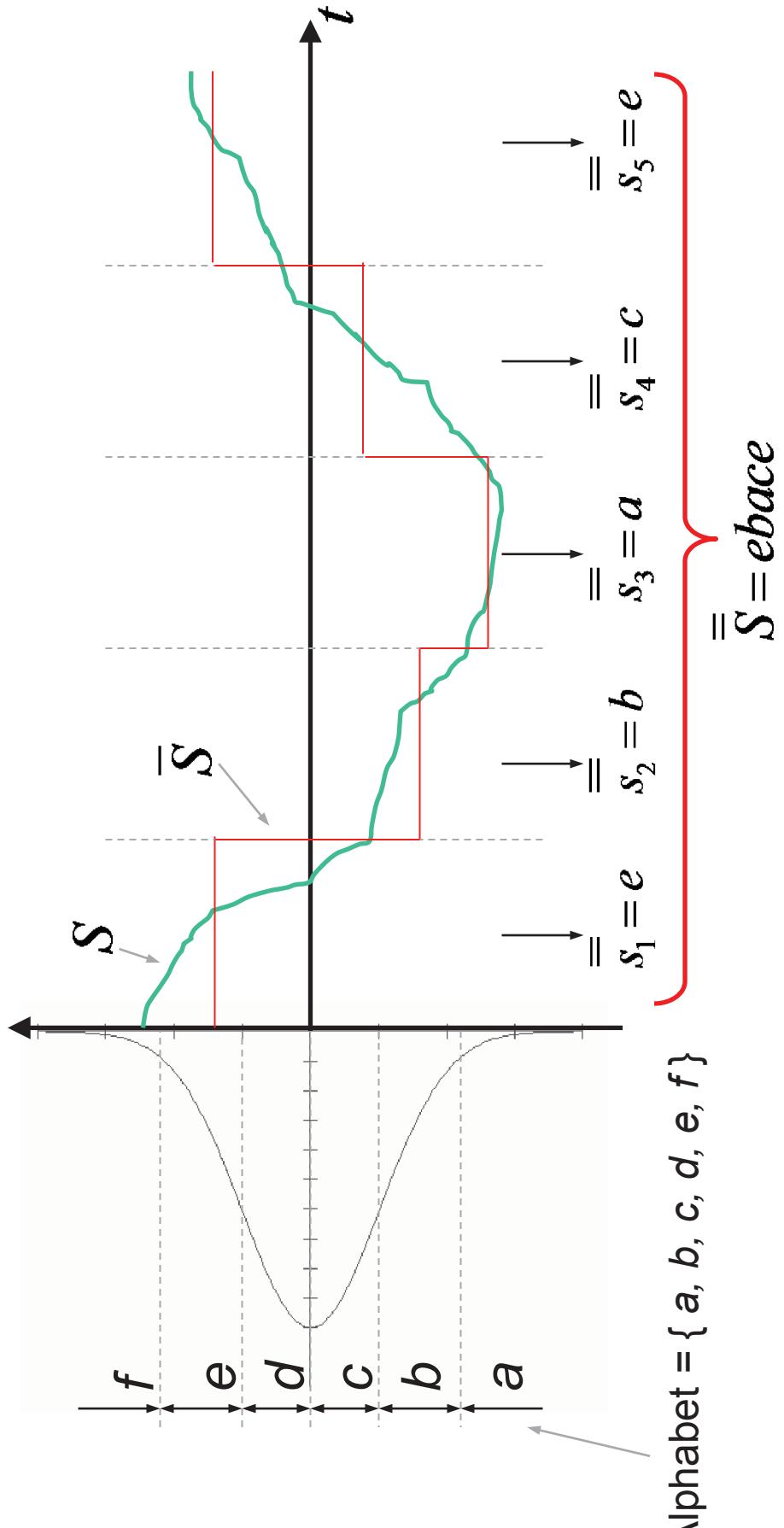
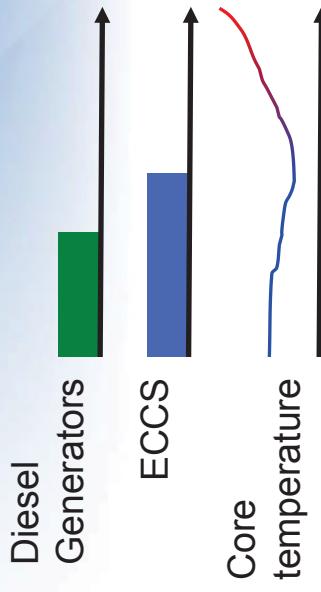
$$d_{DTW}(Q, C) = \min \left\{ \sqrt{\sum_{k=1}^K w_k} \right\}$$



Warping Window

Symbolic Representation



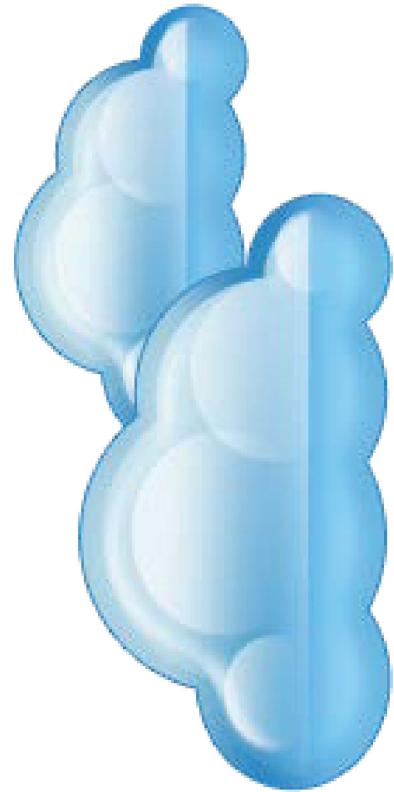


Cloud Technologies for use in Risk Assessment

An introduction to cloud concepts,
architecture, and toolsets

Curtis Smith and Kellie Kvarfordt

August 2013



www.inl.gov



What do we mean by “cloud computing”?

- Wikipedia
 - Cloud computing is a jargon term without a commonly accepted non-ambiguous scientific or technical definition
- National Institute of Standards and Technology (NIST)
 - Cloud computing is a **model** for enabling ubiquitous, convenient, on-demand network access
 - Users have access to a shared pool of configurable computing resources
 - E.g., networks, servers, storage, applications, and services
 - Can be rapidly provisioned and released with minimal management effort or service provider interaction

What do we mean by “cloud computing”?

For our purposes, we'll use the simple definition brought up in a Google Search

cloud computing

Noun

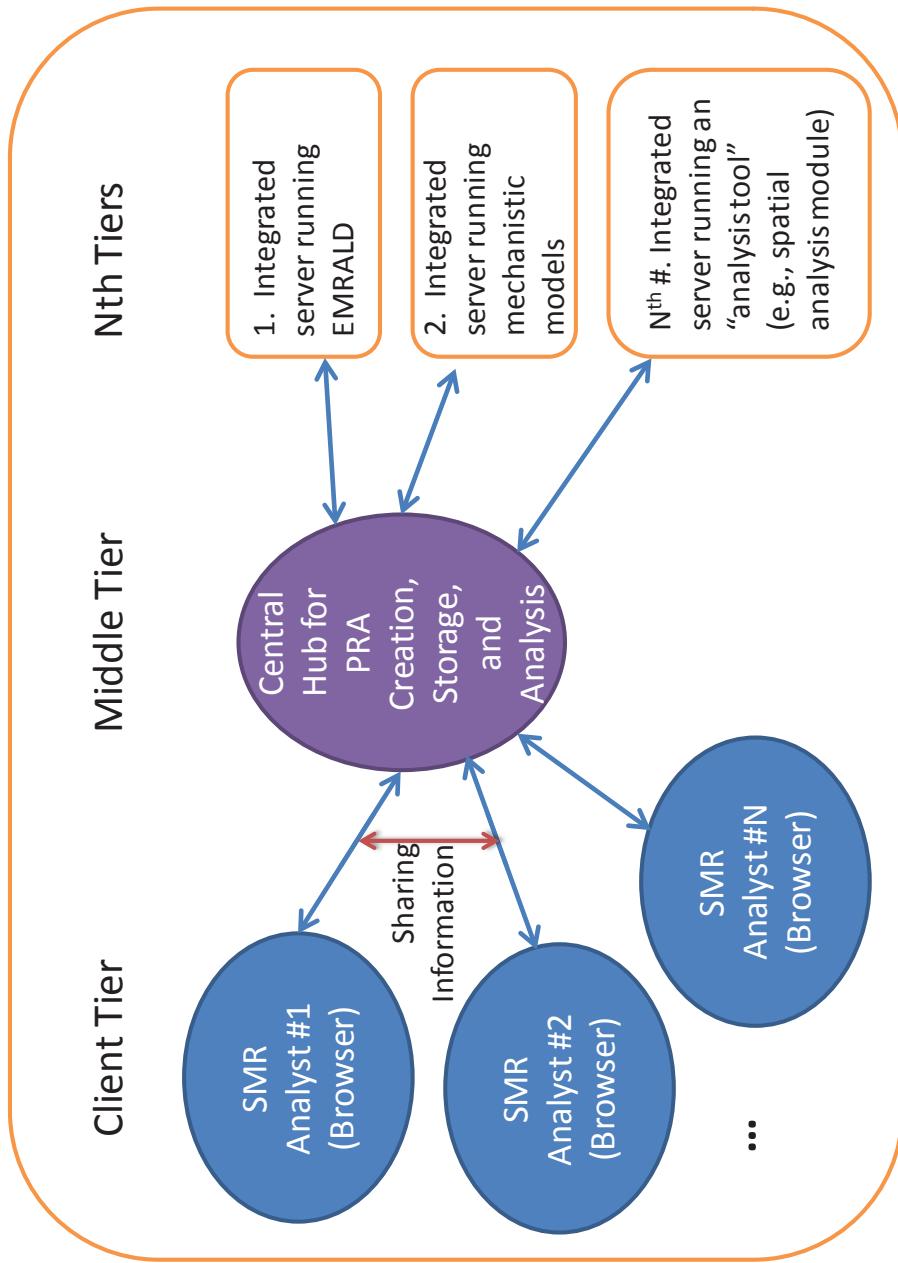
The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server...

The Goal of our Cloud

Enable seamless integration of

data + information + models + tools

SMR PRA Cloud-based Tool Conceptual Design

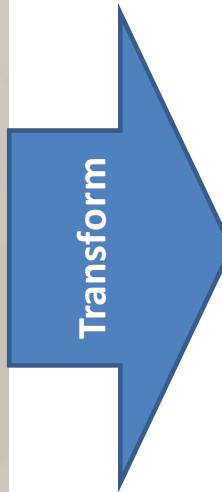


Data Transformation



Objects are stored once

Transform 3D picture of pipe to XML representation.

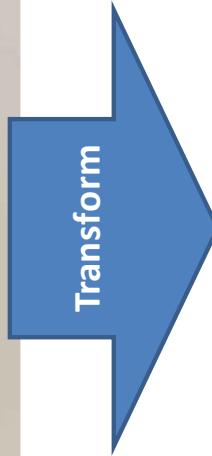


Simplified XML representation:

```
<pipe>
  <material>
    <properties length = '22' metal='iron'>
      </properties>
    </material>
  </pipe>
```

Data Transformation

Transform 3D picture of pipe to mathematical equation for flow



$$q - w = \left(u_2 + g z_2 + \frac{p_2}{\rho} + \frac{v_2^2}{2} \right) - \left(u_1 + g z_1 + \frac{p_1}{\rho} + \frac{v_1^2}{2} \right)$$

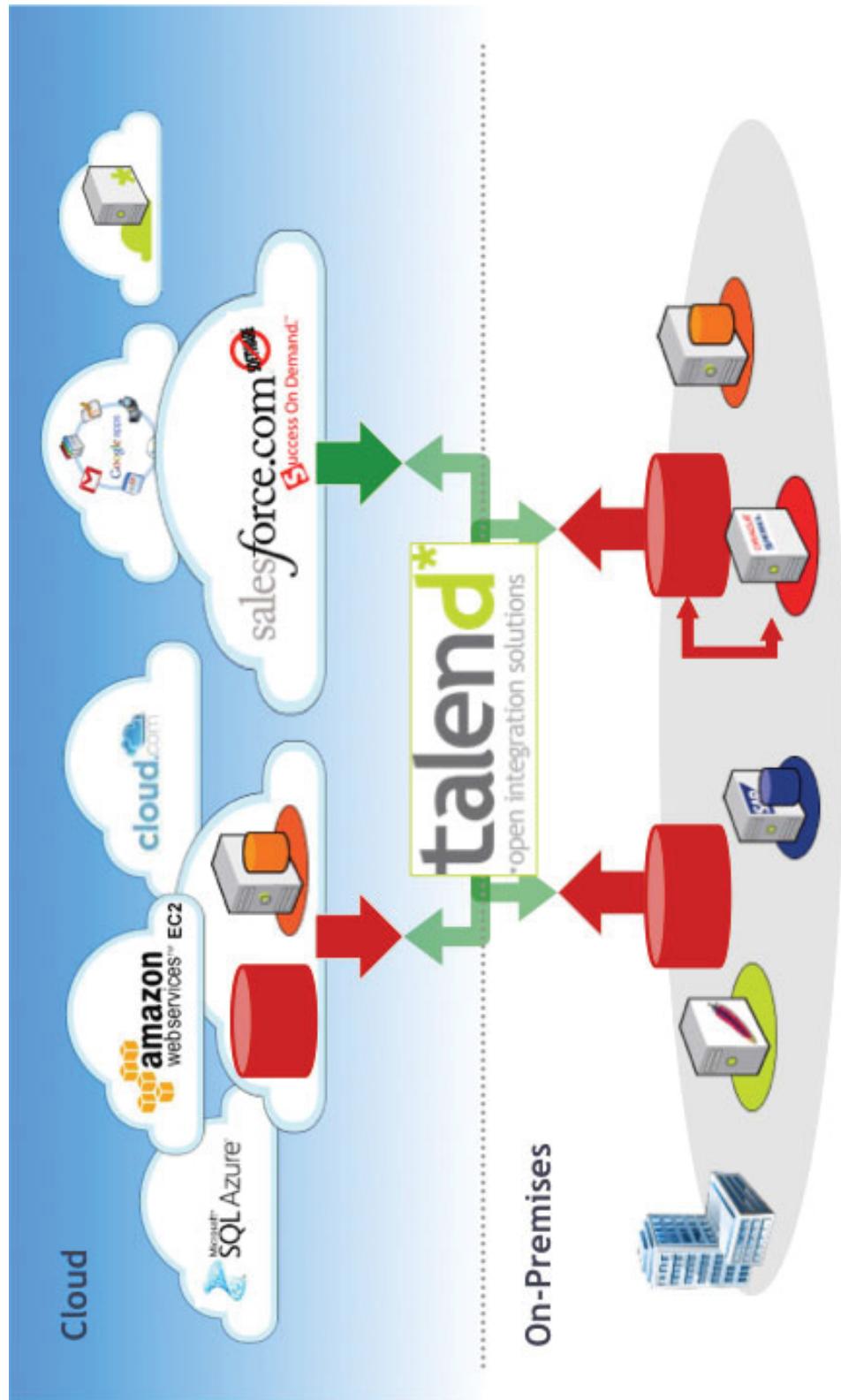
Software integration module examples

Software Module	Description	Maturity Level	Open Source?
SAPHIRE	Software to solve static cut set based logic models	High	No, the source is available for use at the INL
RELAP	Software to solve T-H conditions	High	No, the source is available for use at the INL
MySQL	Software to manage data storage in a full relational database	High	Yes
EMERALD	Software to solve reliability-based simulation models	Low	Yes
Jini	Software to develop distributed systems consisting of network services and clients.	High	Yes
WebGL	Software to display advanced a graphical 3D environment in an Internet browser	High	Yes
id Tech 4 Engine	Software to create and use a graphical 3D environment and physics engine	High	Yes
OpenBUGS	Software to perform Monte Carlo-based Bayesian updating	Medium	Yes

Where will the SMR PRA Cloud live?



Cloud Tool Possibilities



Cloud Tool Possibilities @ National Labs

The 22 U.S. DOE national laboratories and plants that comprise the nation's federal scientific research and defense systems provide strategic scientific and technological capabilities.

Their collective goal is to meet the nation's challenges and priorities in these areas, which often reach beyond the scope of academia and private industry; and also to ensure that our government has access to these crosscutting discoveries and innovations.

Department of Energy National Laboratories and Plants Leadership in Cloud Computing



<http://www.nrel.gov/docs/fy13osti/56143.pdf>

Cloud Tool Set Capabilities

- Standard components to use as building blocks
 - Examples: Use a preconfigured wiki component; layout managers
- SDKs and APIs that provide higher levels of abstractions
 - Example: Allow programmers to write to cloud storage as easily as a local or network drive
- Patterns that solve common, generic problems
 - Example: How to “talk” to a different system?
 - Request and Reply
 - Fire and Forget
 - Batch Processing

Benefits of Cloud Computing

- Access from anywhere
- Collaborate
- Track revisions
- Store and use latest data/models/tools
- Integrate multiple applications & tools
- Scale (as computational power increases – add resources)

Cloud Collaboration Example



WIKIPEDIA
The Free Encyclopedia

Article Talk

The Bahamas

From Wikipedia, the free encyclopedia
(Redirected from Bahamas)

Read

"Bahama" and "Bahamas" redirect here. For other uses, see [Bahama](#) (disambiguation).

Main page

Contents

Featured content

Current events

Random article

[Donate to Wikipedia](#)
[Wikimedia Shop](#)

Interaction

Help

About Wikipedia
Community portal

Recent changes

Contact page

Toolbox

Print/export

Languages

Achéh

Afrikaans

Alemannisch

አማርኛ

አማርኛ

Read

Edit source

View history

Search

The Bahamas

From Wikipedia, the free encyclopedia
(Redirected from Bahamas)

Read

Edit source

View history

Search

The Bahamas: Revision history

From year (and earlier): 2013 F

View logs for this page

For any version listed below, click on its title to view the revision.

External tools: Revision history statistics
(cur) = difference from current version, (pr) = difference from previous version, (newer | oldest) View (newer | older) 5

Compare selected revisions

Interaction

Help

About Wikipedia
Community portal

Recent changes

Contact page

Toolbox

Print/export

Languages

Achéh

Afrikaans

The Bahamas



WIKIPEDIA

The Free Encyclopedia

Read

Edit source

View history

Search

Editing The Bahamas

You are not logged in. Your IP address will be publicly visible if you make any edits associated with a user name, among other benefits.

Content that violates any copyrights will be deleted. Encyclopedic content must be verifiable, redistributed by anyone, subject to certain terms and conditions.

B I

[{{redIRECT|Bahama|Bahamas}}](#)

[{{User:dmv/dates|date=May 2013}}](#)

[{{PP-move-indef}}](#)

[{{Infobox country}}](#)

Common_name = the Bahamas

Conventional_long_name = Commonwealth of the Bahamas

Image_flag = Flag of the Bahamas.svg

Image_coat = Coat of arms of the Bahamas.svg

Image_map = LocationBahamas.svg

National_motto = Forward, Upward, Onward, Together!

National_anthem = "[[March On, Bahamaland]]"

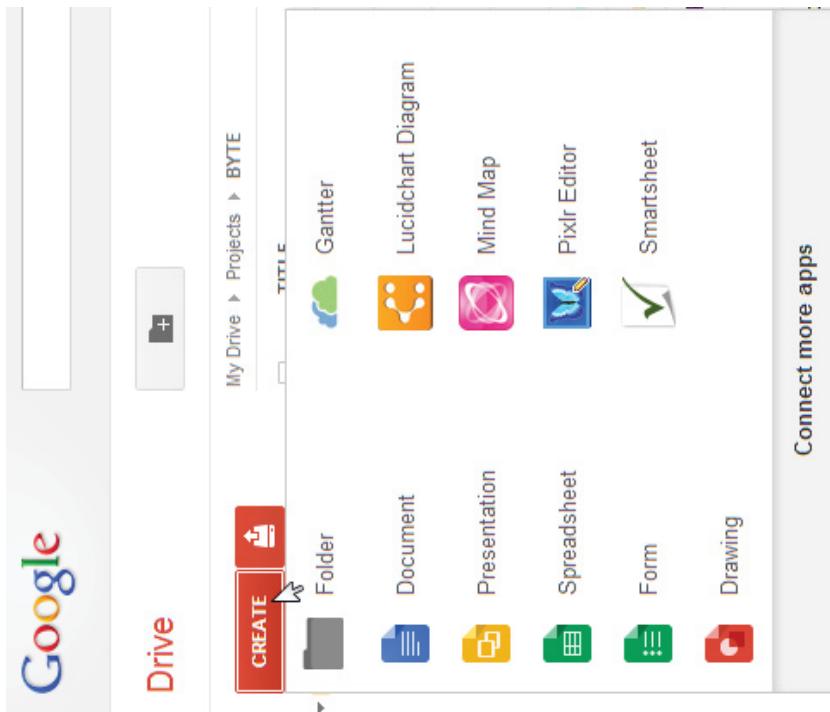
Royal_anthem = "[[God Save the Queen]]"

Official_languages = [[English language|English]]

Ethnic_groups = {{Inowrap|{{vtable|10.7% Not Stated|10.4% Asian People|Asian Indian}}}};

Ethnic_groups_year = {{Inwrap|10.4em|<ref name="http://statistics.bahamas.gov.bb/2011census/2011census.htm#DemographicProfile">}}

Cloud Storage Examples



The screenshot shows the Google Drive interface. At the top, there's a navigation bar with 'My Drive' and 'Projects'. Below it, a 'CREATE' button with a plus sign is highlighted with a red arrow. A dropdown menu lists several options: 'Folder', 'Document', 'Presentation', 'Spreadsheet', 'Form', and 'Drawing'. To the right of these, there are icons for 'Gantter', 'Lucidchart Diagram', 'Mind Map', 'Pixel Editor', and 'Smartsheet'. At the bottom right of the interface, a link says 'Connect more apps'.

Google Drive

Drive

CREATE

My Drive > Projects > BYTE

Folder Document Presentation Spreadsheet Form Drawing

Gantter Lucidchart Diagram Mind Map Pixel Editor Smartsheet

Connect more apps

cloud drive

Microsoft SkyDrive.

Dropbox

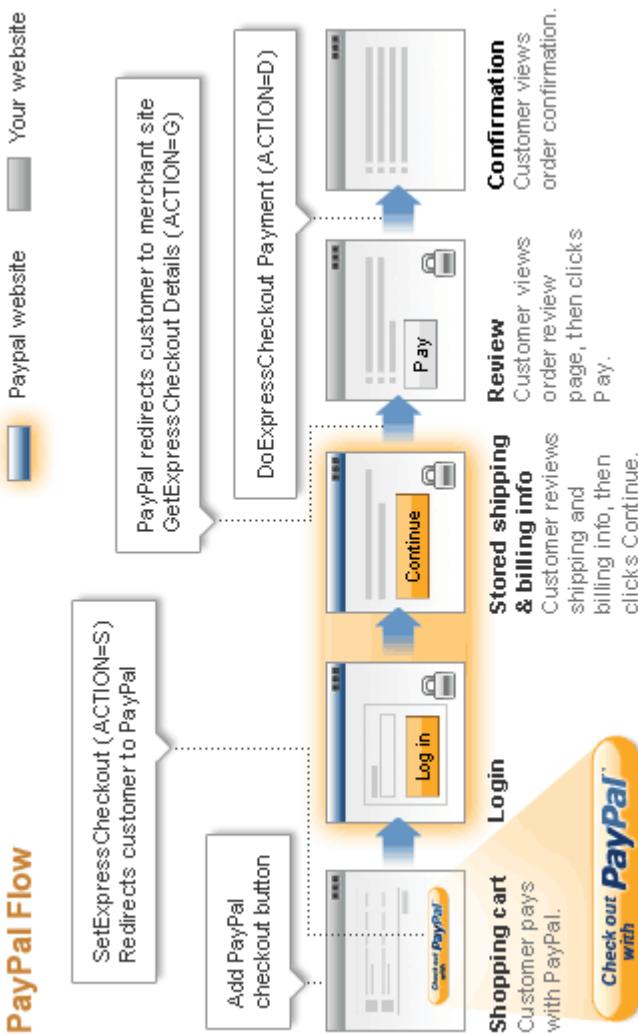
VS:

Google Drive

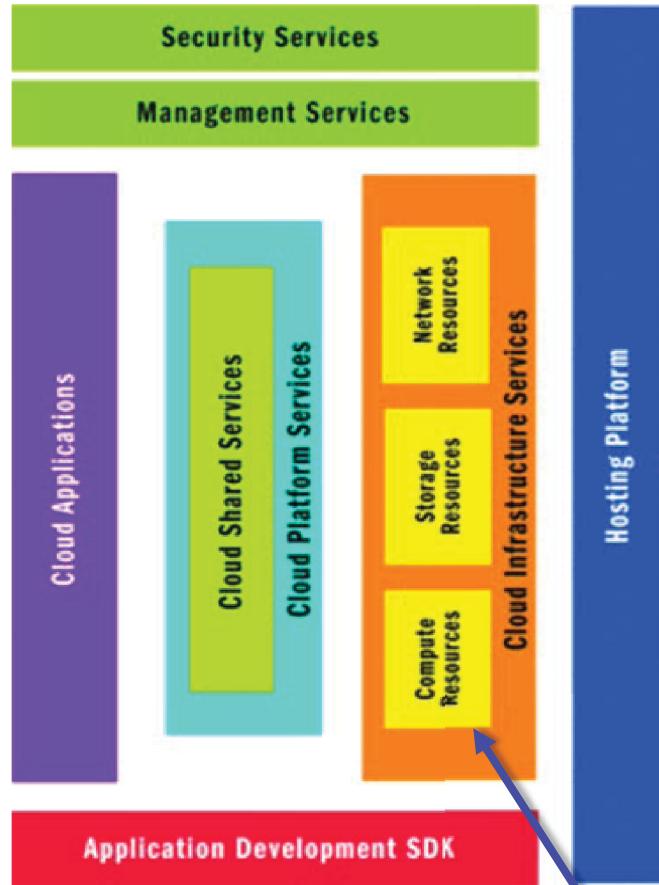
iCloud

Cloud Integration Example

Payments systems, such as Paypal and Google Checkout

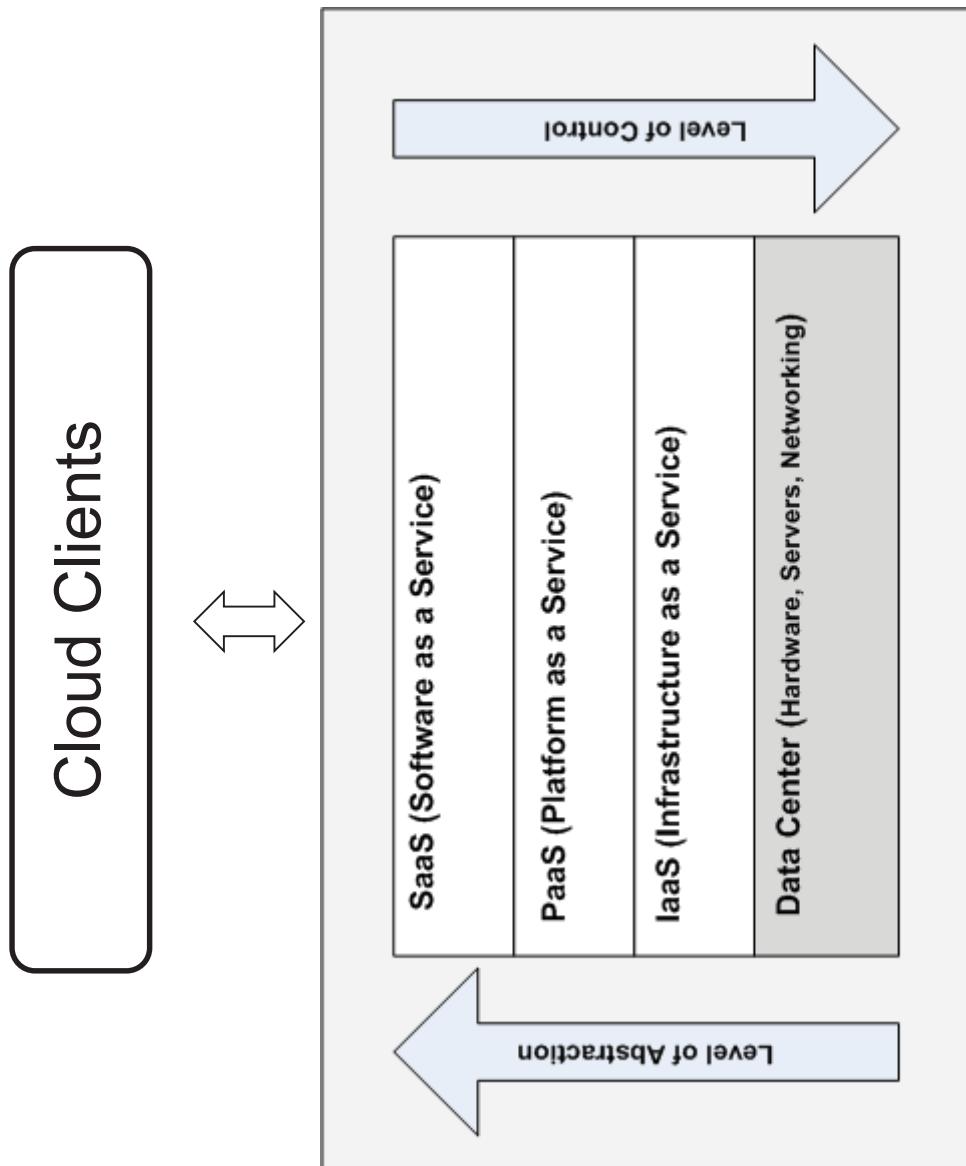


Components of a Cloud



Google Compute Engine

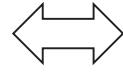
Cloud Service Models



Cloud Clients

Cloud Clients

User will use a modern browser such as recent versions of



- Chrome
 - Firefox
 - Internet Explorer 9
 - Safari
- to access...

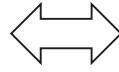
SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)
Data Center (Hardware, Servers, Networking)

Software as a Service (SaaS)

(User level tools)

Cloud Clients

Examples



- Gmail
- Google Docs (documents, spreadsheets, presentations)
- Office 365
- Draw.io

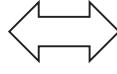
SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)
Data Center (Hardware, Servers, Networking)

Platform as a Service (PaaS)

(Developer level tools)

Cloud Clients

Examples



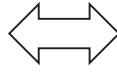
- Google AppEngine
- SalesForce
- Windows Azure Cloud Services

SaaS (Software as a Service)	PaaS (Platform as a Service)	IaaS (Infrastructure as a Service)	Data Center (Hardware, Servers, Networking)
------------------------------	------------------------------	------------------------------------	---

Infrastructure as a Service (IaaS) *(System manager tools)*

Cloud Clients

Examples



IaaS (Infrastructure as a Service) (Compute, Storage, Network)

- Amazon Elastic Compute Cloud (EC2)
- Google Compute Engine
- IBM CloudBurst

SaaS (Software as a Service)

PaaS (Platform as a Service)

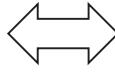
IaaS (Infrastructure as a Service)

Data Center (Hardware, Servers, Networking)

Data Center (Hardware, Servers, Networking)

Cloud Clients

Examples



- Virtual Machines
- Servers
- On-Premises Network
- Storage

SaaS (Software as a Service)
PaaS (Platform as a Service)
IaaS (Infrastructure as a Service)
Data Center (Hardware, Servers, Networking)

(Data center services can be provided by IaaS)

Challenges of Cloud Computing

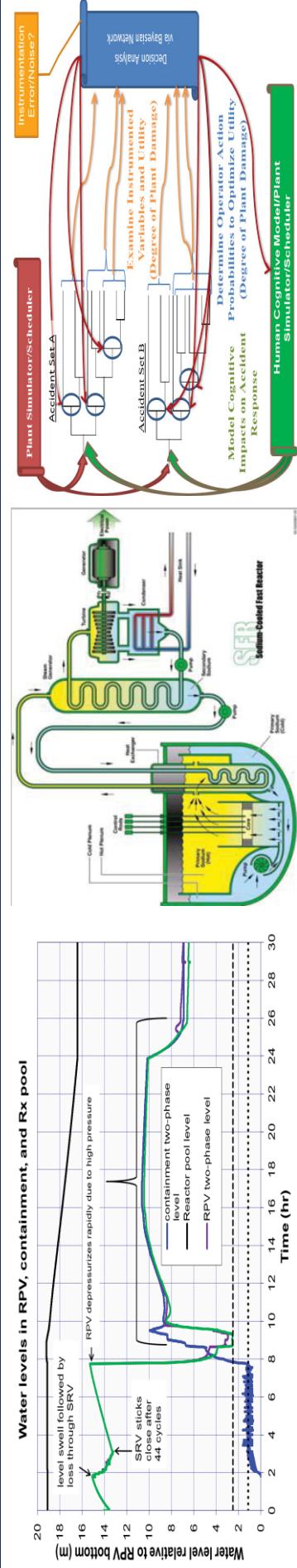
- Security requirements must be met
 - Encryptions and passwords
- Integration is non-trivial
 - Tools exists and are becoming more plentiful and powerful
- Learning curve
 - Requires profession programmers
- Possible cloud tools lock-in
 - Export capabilities (e.g., XML) of data to neutral formats

Conclusions

- From the DOE “Leadership in Cloud Computing” report
 - Cloud computing is here and a readily available resource for organizations
 - Varying degree of movement to the cloud; there is not one solution
 - All organizations highlighted are working toward incorporating the cloud into their IT strategic plans and DOE is making this transition more efficient by enabling the rapid adoption and usage of cloud services
- From the Magellan Report on Cloud Computing for Science
 - Cloud approaches provide many advantages
 - Cloud computing can require significant initial effort and skills
 - Key economic benefit of clouds comes from the consolidation of resources across a broad community, which results in higher utilization, economies of scale, and operational efficiencies
 - DOE should work with the DOE HPC centers and DOE resource providers to ensure that the expanding needs of the scientific community are being met



Exceptional service in the national interest



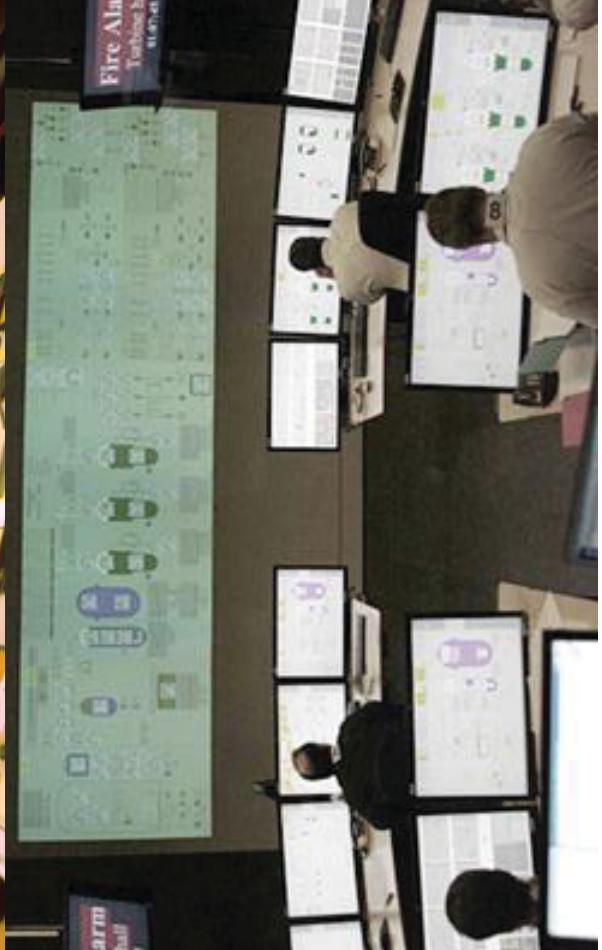
Risk-Informing Incident Management Guidelines

Timothy Wheeler, Dr. Katrina Groth, Dr. Matthew Denman
Risk and Reliability Analysis
Presented to aSMR PRA Technical Exchange Meeting
August 22, 2013

Outline

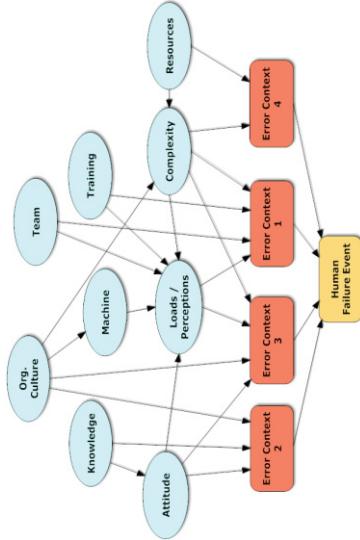
- Establish the difference between Risk-Management and Risk-Analysis.
- Describe the challenges SMRs present to state-of-the-art of risk-assessment and regulation
- Describe the value of risk-informed analysis when analyzing safety of SMRs
- Describe how the transition from the FY13 work package to the FY14 work package

Photo Credits:
Top: Tennessee Valley Authority
Bottom: Halden Reactor Project



Risk Management vs Risk Analysis

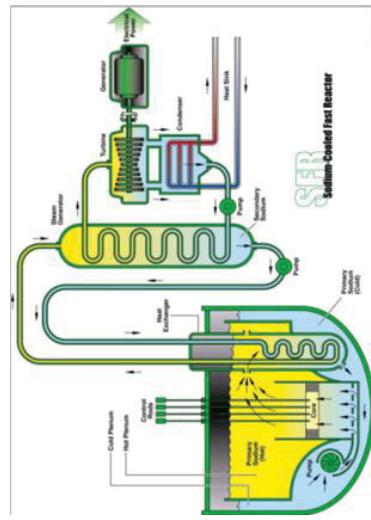
- Risk Analysis gives us an understanding of the nature, magnitude, and consequences associated with human and natural activities.
 - e.g., Statistics helps inform in the presence of uncertain but static conditions.
- Risk Management uses the results of Risk Analysis to facilitate decisions regarding risk
 - Helping operators make decisions in changing conditions with unknown parameters.
- Both perspectives are necessary for comprehensive safety strategies.



Challenges SMRs present to state-of-the-art of risk-assessment and regulation

Regulatory and Risk Assessment challenges for SMRs

- Passive systems are not compatible with current regulatory infrastructure.
- SMR industry will seek regulatory exemptions from many licensing criteria.
- Both risk analysis and risk-management will play a key role in establishing the safety case for regulatory exemptions.
- Traditional static fault-tree/event-tree methods have limited capability for:
 - passive system performance
 - assessment of alternative staffing strategies



In 2009, NRC set forth expectations for advanced PRA and accident sequence modeling [1].

- **Reduce modeling simplifications (i.e., enhanced phenomenological modeling).**
 - Address methodological shortcomings exposed through the NRC's State-of-the Art Reactor Consequence Analyses (SOARCA) project.
 - e.g., more realistic modeling of source terms.
 - **Improve treatment of human interaction and mitigation.**
 - **Make process and results more understandable.**
 - Utilize advances in computational capabilities,
 - **Characterize uncertainty.**
- NRC – in light of Fukushima – is placing greater emphasis on demonstration of severe accident management and mitigation. (Level 2 and 3 PRA)

■ [1] D. Helton, "Scoping Study on Advancing Modeling Techniques for Level 2/3 PRA," U.S. Nuclear Regulatory Commission, May 2009.
Available via the US NRC's Agency-wide Document Access and Management System at accession no. ML091320454.

Industry Objectives that will Challenge State-of-the Art Risk Assessment

Desired Licensing Changes	Industry Justification
<ol style="list-style-type: none">1. Smaller exclusion zone<ul style="list-style-type: none">• Simpler emergency planning2. Reduced Staffing Requirements<ul style="list-style-type: none">• Operational• Security• Maintenance• Multi-unit operations	<ol style="list-style-type: none">1. SMRs are inherently consequence-free<ul style="list-style-type: none">• No off-site source term• Larger safety margins2. Passive safety systems make SMRs “walk-away” safe.<ul style="list-style-type: none">• Fewer operators needed• Less attractive to adversaries

Exemption requests may prove challenging

- Preliminary SMR source term calculations for NRC show:
 - SMR reactor core inventories could potentially exceed NRC dose criteria during an accident or sabotage.
- Containment bypass is feasible through containment penetrations and interfacing systems
 - Claims of extraordinarily low or no source terms must be rigorously validated.
 - Can multiple units increase the site source term?
- Management of Beyond-Design-Basis Accidents may-not be achieve solely with passive systems
 - Will require operator intervention and use of non-passive systems.
 - Investment protection and protection of public health and safety
 - What is the cognitive load on an operator during an accident?
 - Multi-tasking on multiple units?
 - Can human action unintentionally interfere with passive cooling?

Summary of SMR Risk Assessment Challenges

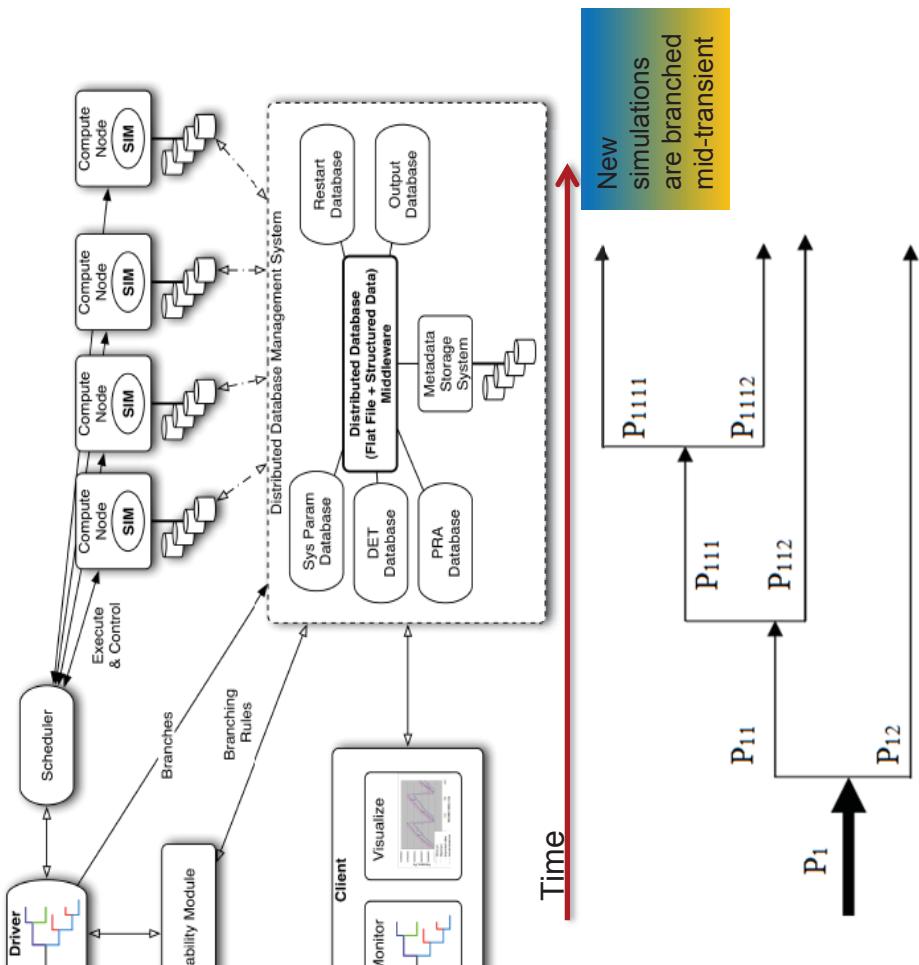


- SMRs provide many safety advantages over traditional LWRs, but justifying regulatory changes will be difficult
- The fundamental decision problems posed by SMR induced regulatory changes may not be answerable by traditional metrics such as
 - Core Damage Frequency (CDF) and
 - Large Early Release Frequency (LERF)
- New problems demand new analysis techniques integrating all of the following:
 - Safety Analysis
 - Cognitive psychology
 - Decision Support

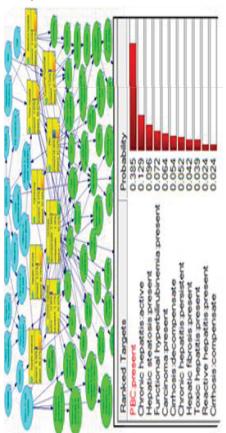
The promise of risk-informed analysis for analyzing the safety case for SMRs

Discrete-Dynamic-Event-Trees (DDET)

- DDET is a methodology for exploring large spectrum of possible accident scenarios.
 - Simulates multiple accident sequences by branching based on physics calculations.



How Bayesian Networks (BNs) work



The generic knowledge base (BN) contains variables and [prior] probabilities

- Components of the system
- How possible defects manifest through symptoms, test results, error messages etc.

Observations:

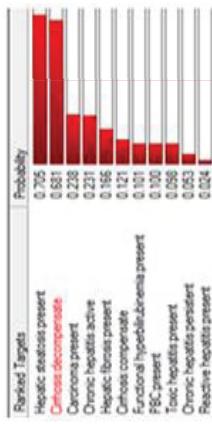
- Sex: male
- Irregular liver: present
- History of alcohol abuse: present
- Platelet count: 0-99

Users make observations about known symptoms or test results for a specific situation/person

Parent	$Pr(a)$	$Pr(\bar{a})$
$Pr(b)$	$Pr(b a)$	$Pr(b \bar{a})$
$Pr(\bar{b})$	$Pr(\bar{b} a)$	$Pr(\bar{b} \bar{a})$

$$P(X_1, X_2, \dots, X_n) = \prod_i P(X_i | \text{Par}_G(X_i))$$

Observations are propagated (forward and backward) through the network to provide posterior probability of every node



Posterior probability can be used for reasoning (e.g., ranking diseases, selecting tests, calculating value of information for tests)

Examples of uses of Bayesian Networks (BNs) to support diagnosis activities in a range of industries

- Medicine
 - Diagnosis of liver disorders
 - Congenital heart disease diagnosis
 - Preliminary Diagnosis of neuromuscular diseases
 - System for insulin adjustment for diabetics
 - Diagnosis of breast cancer
- Business and Management
 - Finance-Fraud/Uncollectible debt collection
- Engineering & Science
 - Expert system based for cattle blood group determination
 - Diagnosis of faults in waste water treatment process

Advanced Risk Analysis and Risk Management Methods can address NRC Expectations and Industry Objectives

- Discrete Dynamic Event Trees (DDET)
 - Reduces model simplification by allowing for the time-dependent aspects of physical phenomena to be realistically modeled – unlike traditional PRA tools.
 - Dynamic modeling of accident progression allows the development of accident sequence pathways to proceed “naturally” based on the evolution of specific plant conditions rather than a priori developed event trees.
- DDET and Bayesian Networks (BNs)
 - Improve modeling of human actions by generating a spectrum of accident progression conditions (DDET) that can be used to facilitate evaluation of optimal incident management strategies (BN).
 - Document the rationale for emergency procedures in the context of specific accident conditions rather than non-transparent expert judgment and opinion.
 - Elevate PRA from a static a priori pre-accident framework to a dynamic real-time decision support tool.
 - Facilitate the propagation of aleatory (random) and epistemic (knowledge) uncertainties into optimal decisions

Managing Severe Incidents are Difficult

Operators faced serious challenges to diagnosis due to human limitations plus information limitations.

Sources of information limitations:

- **Plant Design:** Current sensors were not designed for accident monitoring
- **Poor Guidance:** Lack of procedures and training to guide information gathering and diagnosis
- **Complexity/Dynamics:** Rapid scenario evolution, short response window

Cognitive challenges:

- **Understanding:** Developing a “big picture” from partial information
- **Filtering:** Deciding which information is relevant to the scenario
- **Prioritizing:** Deciding which information is worth expending limited resources to obtain

How are IMGS currently created?



Sandia
National
Labs

- Combinations of expert judgments and Best Estimate (BE) simulations
 - Hidden assumption: Active management is almost always safer.
 - Is this true?
- BE vs Risk-Informed
 - Flaw of Averages – Risks are underestimated in BE calculations
$$f(\bar{x}) \neq \int f(x) x \, dx, \text{unless } f(x) \text{ is linear}$$
 - Severe accidents are not linear.

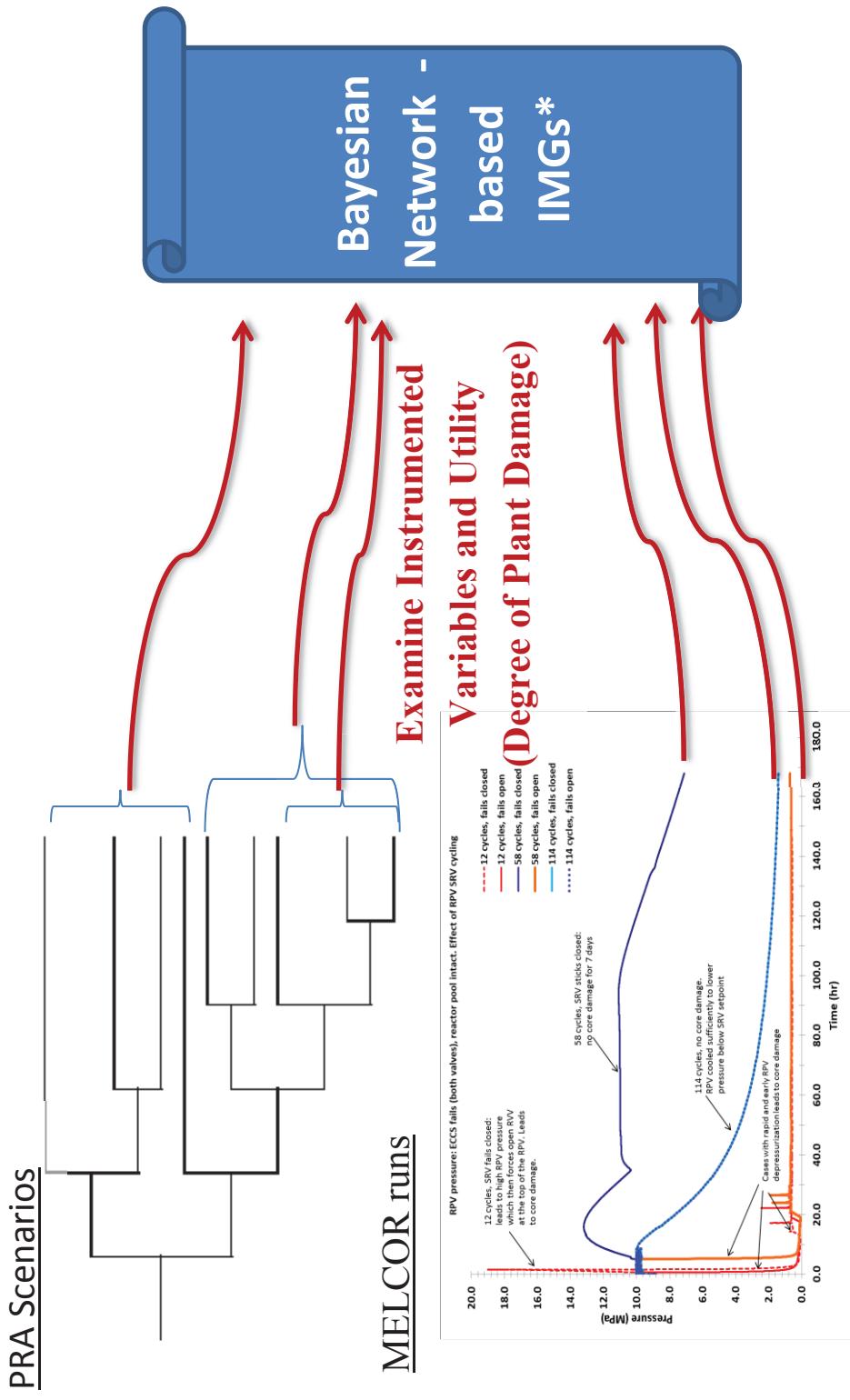
Risk-Management Approach to IMGS



- Risk information can be used to inform accident management in real-time.
 - Advanced PRA simulation models (DDETs)
 - Spectrum of possible accident conditions
 - Decision support models (BNS)
 - Encodes the DDET results in a real-time decision support model
 - Facilitates informed operator response based on frequency and consequences

Smart IMGs in a nutshell

- Build a knowledge base from PRA output & MELCOR runs



*Incident Management Guidelines

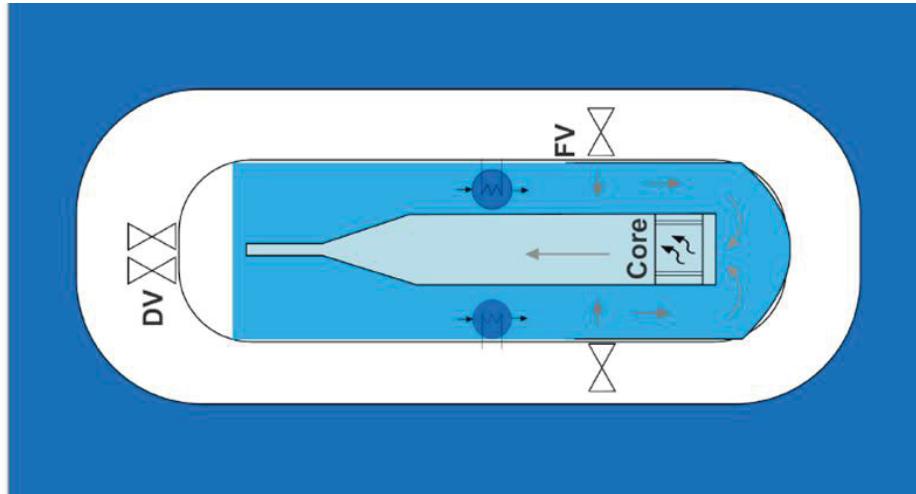
Value of Risk-Informed IMGS



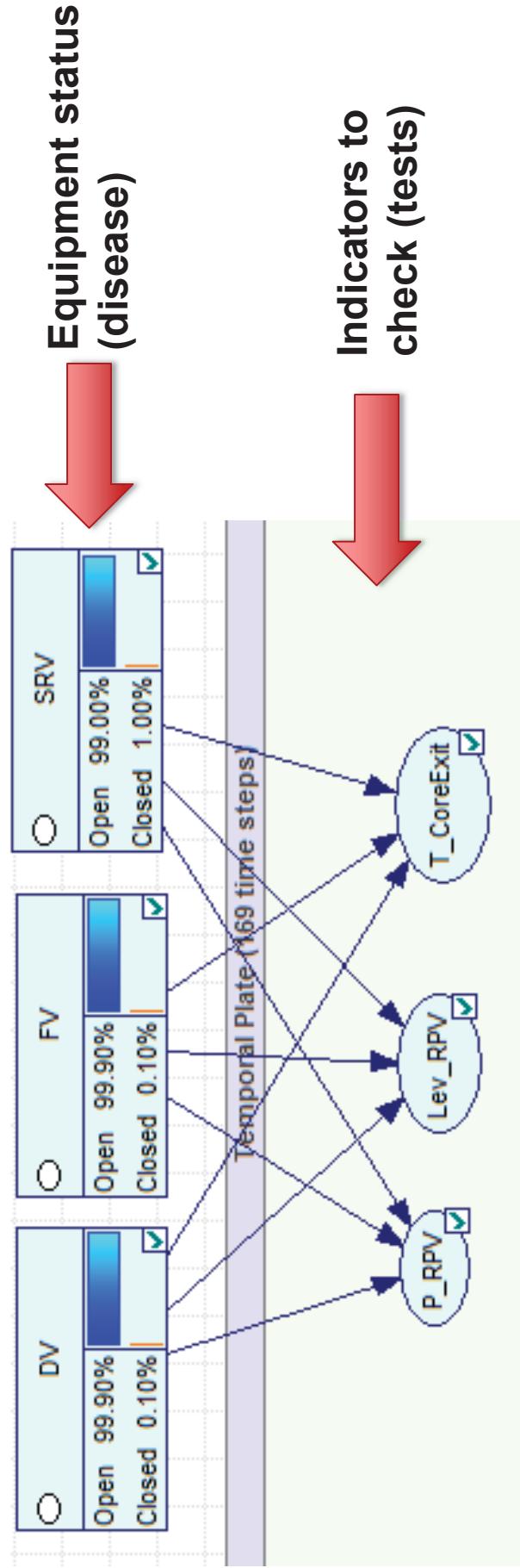
- Use it for real-time reasoning during actual off-normal conditions.
 - Passive safety systems may respond negatively to operator action
 - Avoid unintended consequences by anticipating them with the BN model.
 - Determine what information is useful to the operators
- Simulating an operator's response
 - e.g., for Design Certification prior to existence of plant-specific procedures.

Example system: Generic SMR (FY13)

- Emergency Core Cooling System (ECCS) is a passive system:
 - Depressurization Valves (DVs)
 - Feed Valves (FVs)
 - Safety Relief Valve (SRV)
- Goal: diagnose status of ECCS valves.

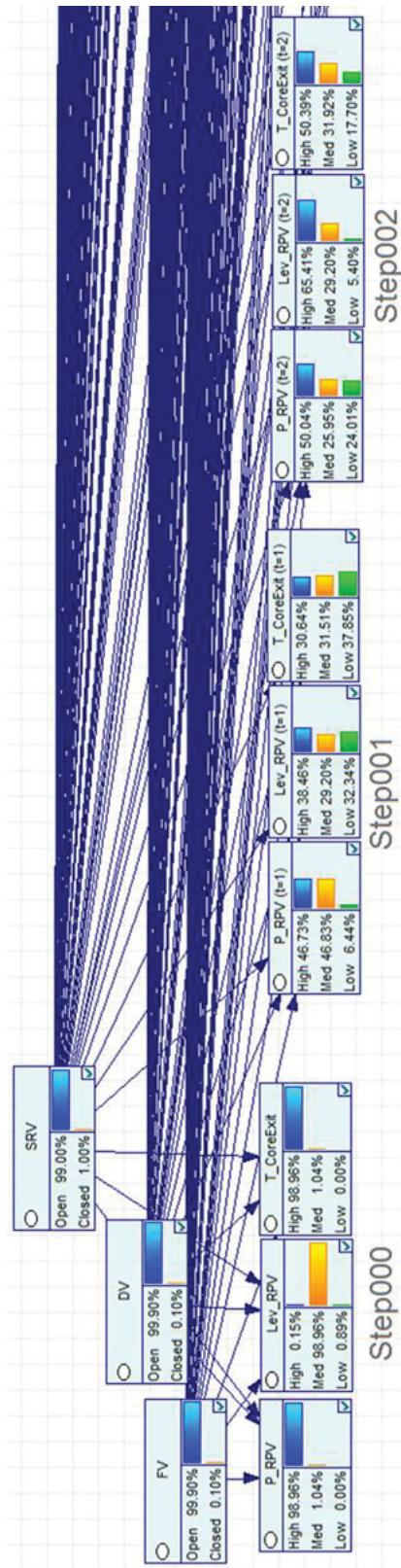


Example BN structure



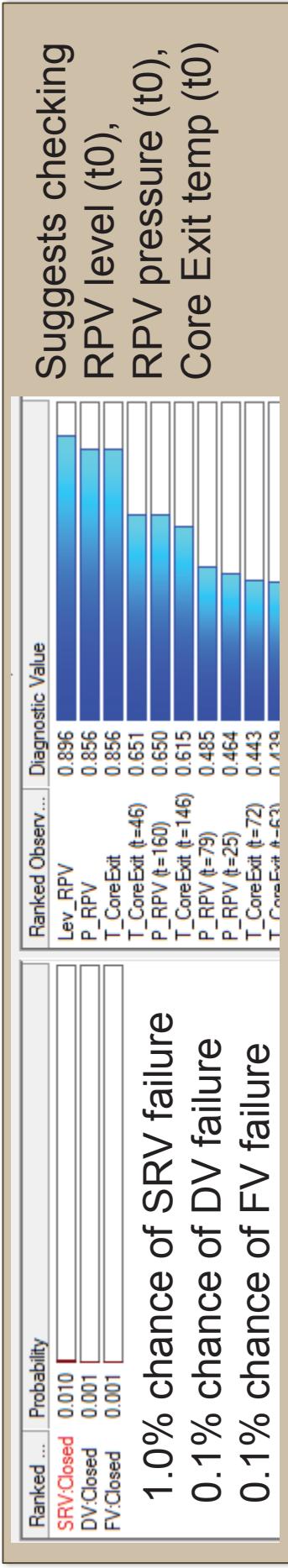
Equipment status
(disease)

Indicators to
check (tests)



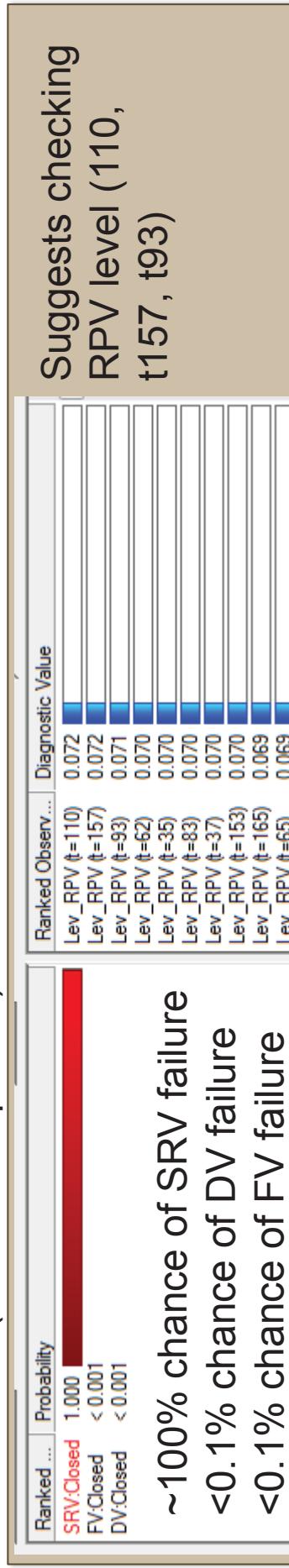
Assisted diagnosis (real-time, iterative)

Prior (Generic day)



Observation: RPV Level (time 0) = low

Posterior (Condition-specific)

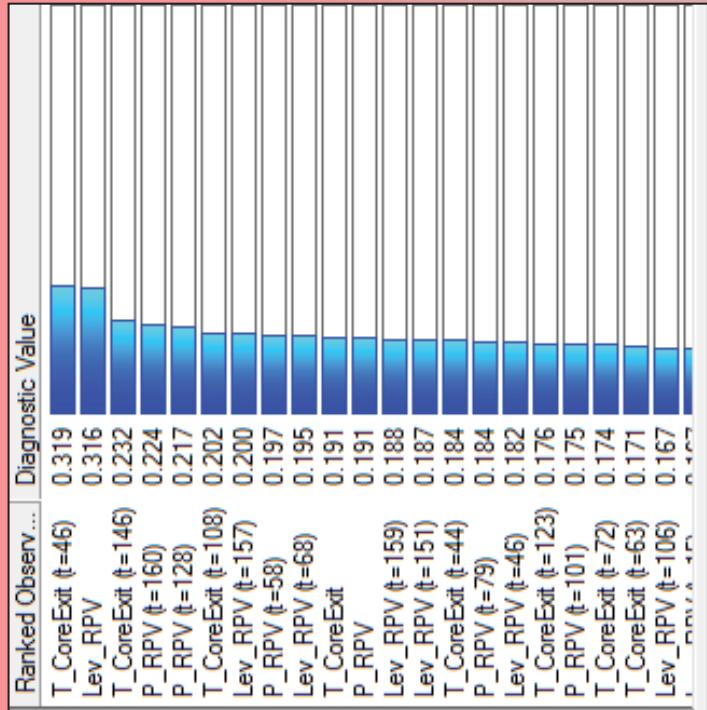


A single key observation dramatically changes belief about ECCS status and value of additional tests

Diagnostic value of tests

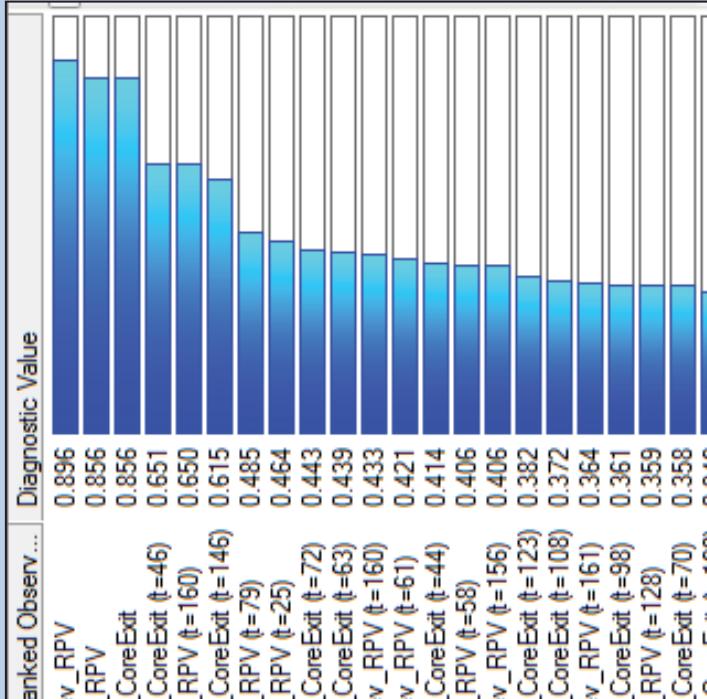


For FV failure



Suggested checks: Core exit temp (t₀), RPPV level(t₀)

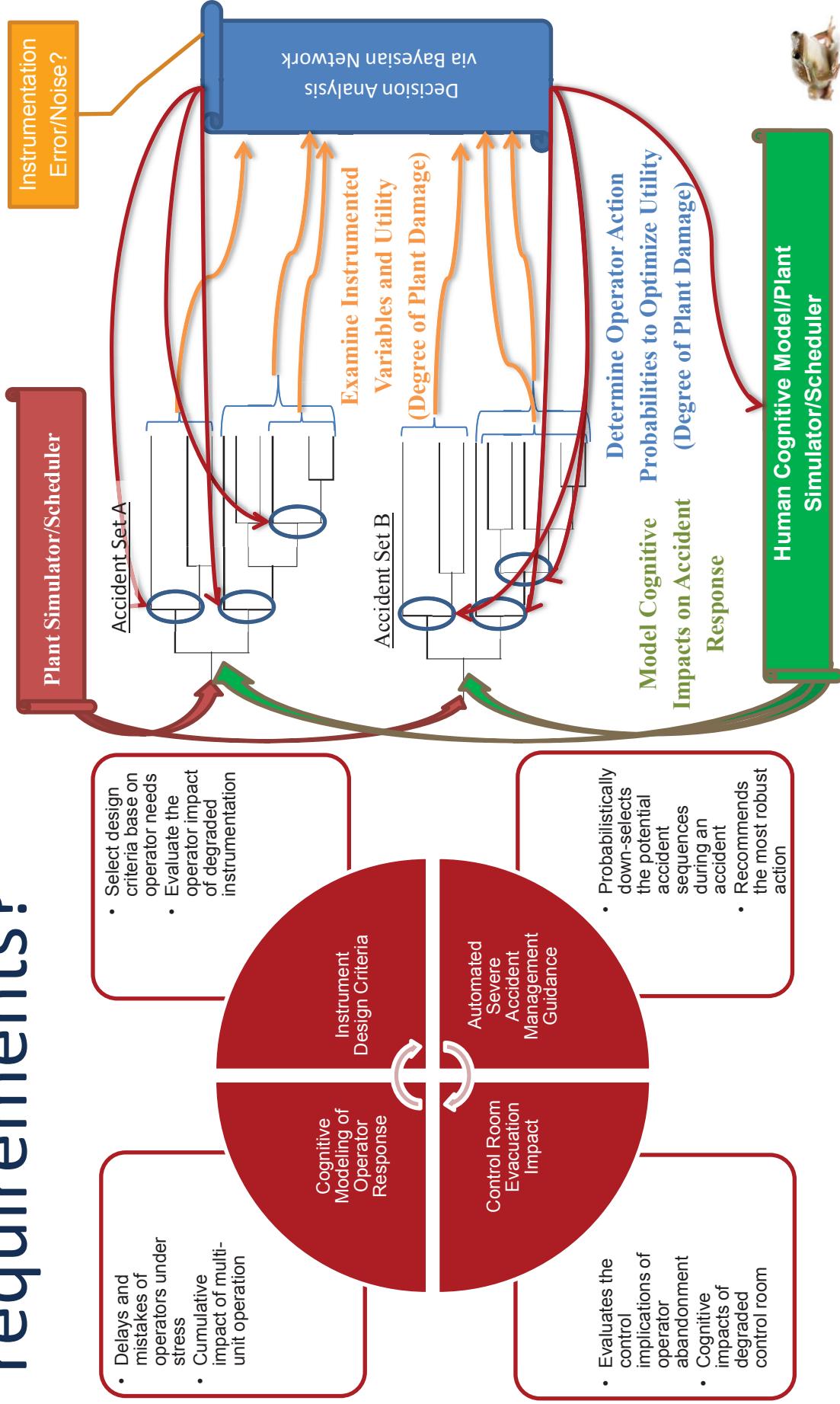
For SRV failure



Suggested checks: RPPV Press(t₀), RPPV level(t₀)

Different tests provide greater diagnostic power for different diseases (and some provide little value for either disease)

How to evaluate staffing requirements?



Transition to FY13 (iPWR) to FY14 (SFR)



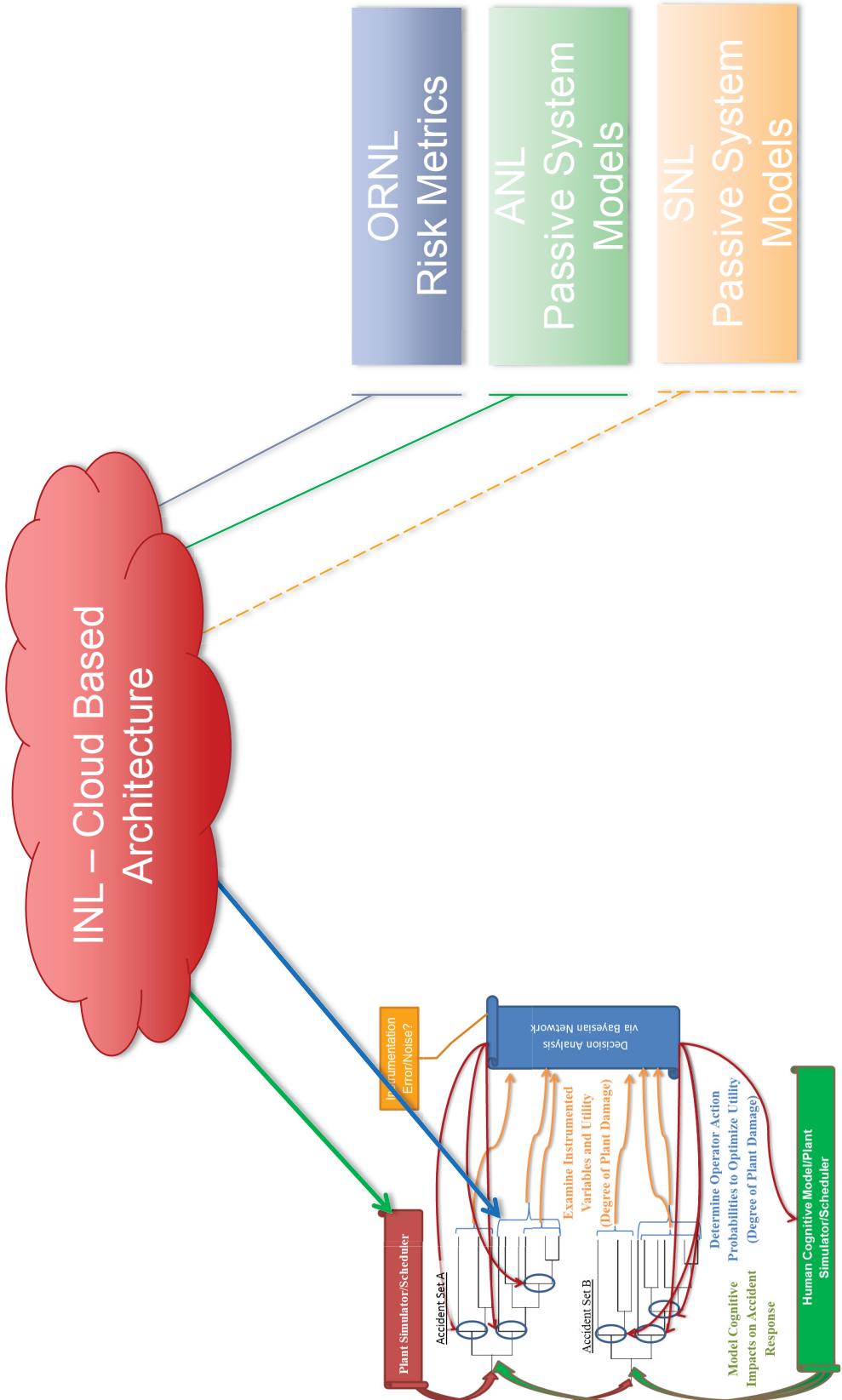
- Consistent analysis approach
 - Identify human intervention that could aid (or hinder) passive system response to challenging incidents.
 - Decision analysis method
 - DDET analysis of passive system response and human intervention
 - BN diagnosis model to down-select accident sequences
 - Selection of risk-metrics
 - Pruned DDET transformation to Decision Tree to determine optimal human action (?)
 - Risk Management benefits
 - IMGs
 - Instrumentation Design Criteria
 - Staffing Evaluation

Note: ANL will be instrumental in assisting this transition by providing a SFR SAS4a model

IMG for SFRs

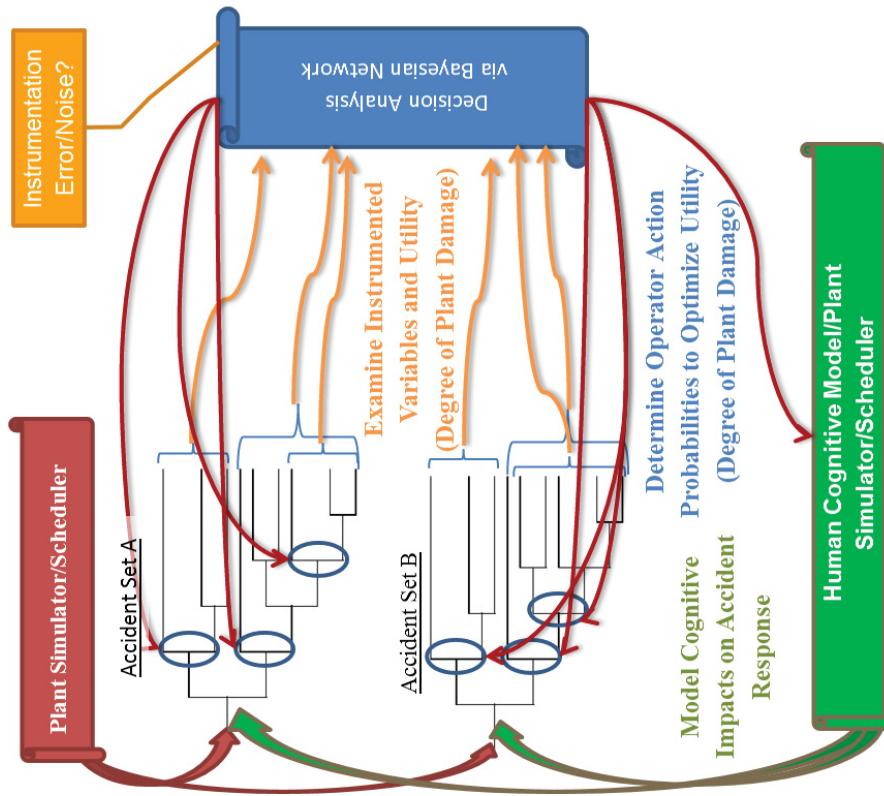
- External event was taken from the ALMR PRA
 - Large earthquake causes a large Unprotected Transient OverPower (UTOP)
 - Operators need to diagnose the accident and decided to:
 - Let inherent safety respond to the accident
 - Increased EM pump flow rate to improve the power to flow ratio and reduce the likelihood of eutectic formation and fuel melting
 - Stressing the pump may cause failure which can worsen the transient (UTOP+LOF)
 - Other RM questions
 - What instrumentation would help the operator?
 - While operators are not necessary to address many unprotected accidents, is there value to their presence or can they only hurt system response?

Integration with other aSMR work packages



Conclusions

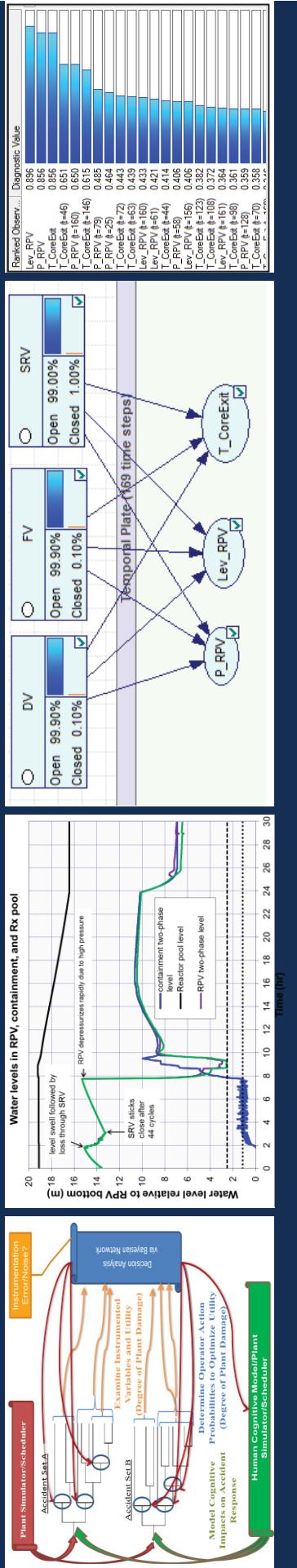
- NRC – in light of Fukushima – is placing greater emphasis on severe accident management.
- DDETs/BNs address NRC PRA expectations.
- DDETs/BNs can be used to evaluate the safety case for aSMRs.
- DDETs/BNs can be used to inform incident management in real-time and provide insight into what information operators need to diagnose the incident.



References

- Smart Procedures
 - Denman MR, Groth KM & Wheeler, TA (2013). "Proof of Principle Framework for risk informed Severe Accident Management Guidelines." *Proceedings of Risk Management for Complex Socio-Technical Systems (RM4CSS) – ANS Winter meeting, Washington DC.*
 - Technical Advance (SD# 12729) "Bayesian network based "smart procedures" development method" (Denman MR, Groth KM, Wheeler TA).
- DDET safety analyses
 - M Denman, J Cardoni, H Liao, T Wheeler, K Groth & D Zamalieva (2013). *Discrete Dynamic Event Tree Capability Study for Advanced Small Modular Reactors-- Proprietary Report.* SAND2013-3352.
 - Denman, MR (2013). "Safety Relief Valve Cyclic Failure Analysis for use in Discrete Dynamic Event Trees.." *Proceedings of PSA2013 -- the ANS Topical Meeting on Probabilistic Safety Assessment, Columbia, SC.*
 - Denman, MR, Cardoni, J, Liao, H, Wheeler, T & Groth, KM (2013). "Discrete Dynamic Event Tree Analysis of Small Modular Reactor Severe Accident Management." *Proceedings of PSA 2013, Columbia, SC.*
 - Liao, H, Cardoni, JN, Denman, MR, Wheeler, TA (2013). "Leveraging existing tools for simulating operator performance in discrete dynamic event trees." *Proceedings of PSA 2013, Columbia, SC.*
- MELCOR: (<http://melcor.sandia.gov/>)

Exceptional service in the national interest



Thank you!

Matthew Denman
Matthew.Denman@sandia.gov
Risk and Reliability Analysis
Sandia National Laboratories



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Backup Slides

Risk-informed “Smart SAMGs” to reduce human failures in NPPs

K. Groth

7 Aug 2013



Sandia
National
Laboratories



*Exceptional
service
in the
national
interest*



U.S. DEPARTMENT OF
ENERGY

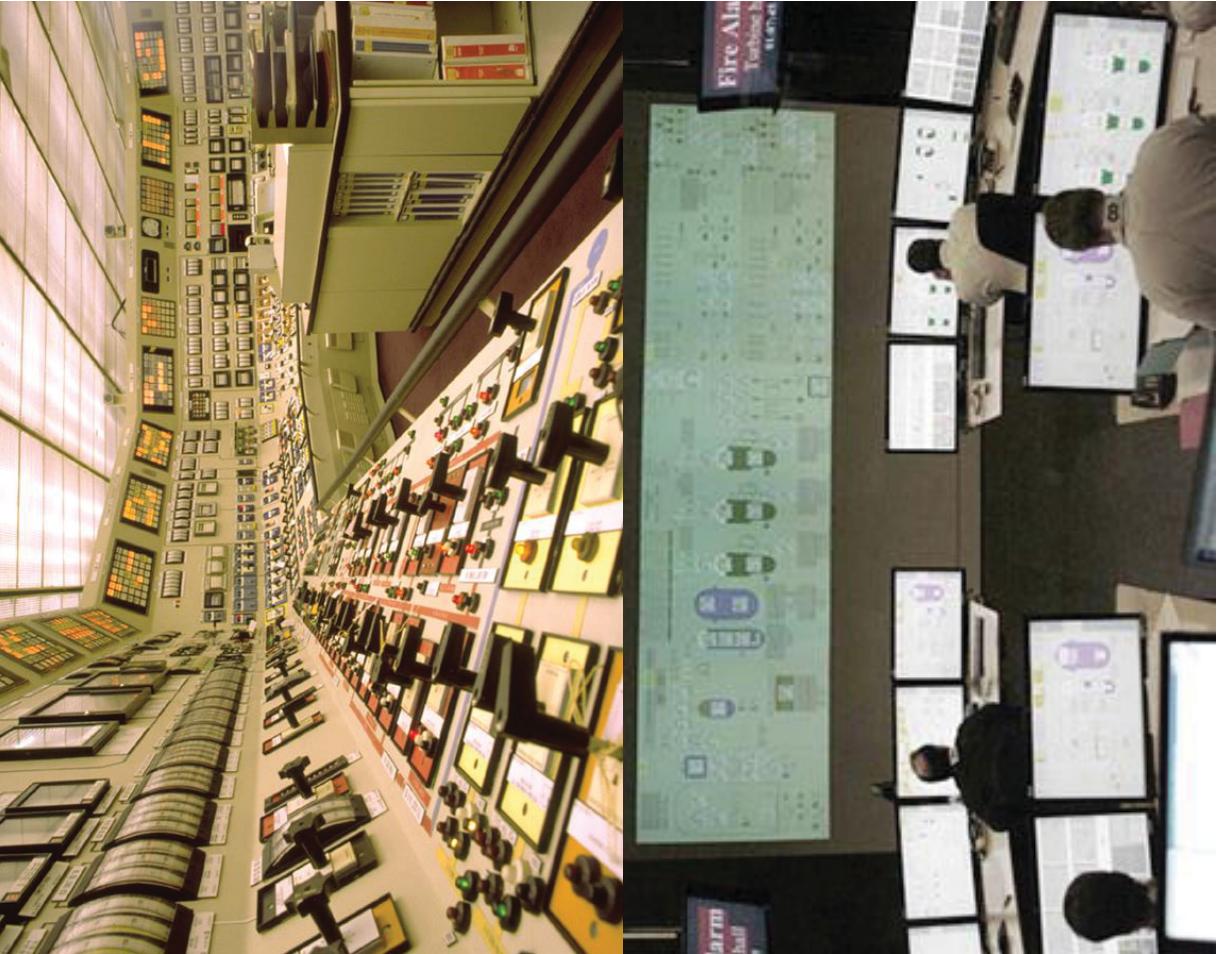


Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Outline

- Goal: Explain my model to Tim, Matt, etc.
- Background
 - Human performance
 - Bayesian Networks for supporting diagnosis
 - “Smart procedures”
- Prototype model demonstration
- Conclusion / Summary

Photo Credits:
Top: Tennessee Valley Authority
Bottom: Halden Reactor Project



Motivations



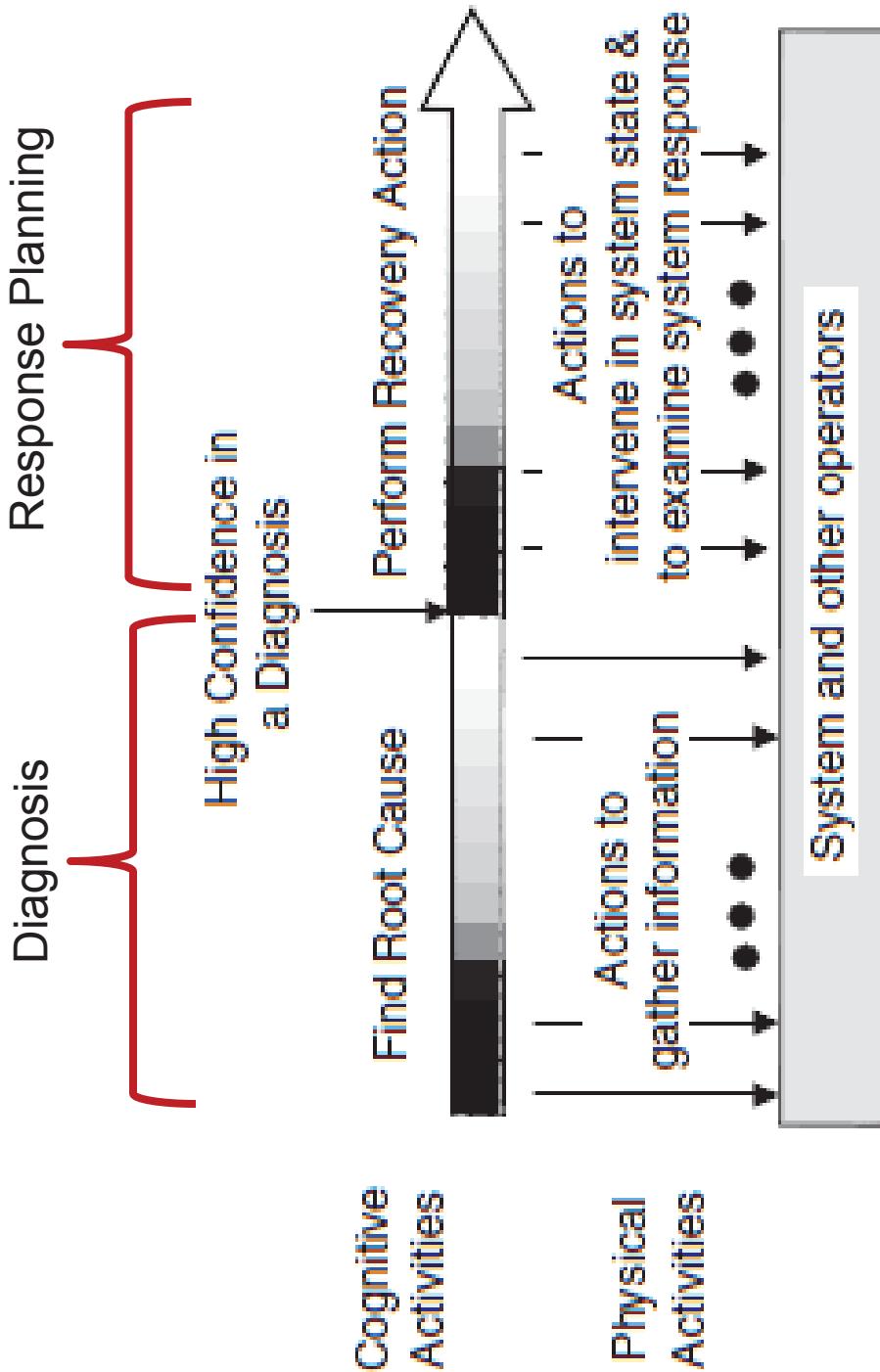
- Immediate: Lack of procedures limits NRC/DOE/NPP ability to develop the safety basis for SMRs
- Broader: During severe accidents, operators faced serious challenges to diagnosis due to human limitations plus information limitations.
- **Hypothesis: Risk information can be used to support decisions beyond the regulatory sphere.**

Objectives



- Immediate: Develop surrogate procedures for SMRs to enable SMR safety analyses
- Broader: Develop and demonstrate methodology for building risk-informed “Smart Procedures”
 - Synthesize best-available information
 - From PRA, system models, plant simulations, etc.
 - ...to provide real-time decision support
 - For operators
 - For NRC, managers, – get everyone on the same page.

Problem Space: Human Response



Characteristics of Humans as Decision Makers

Sandia National Laboratories

Characteristics of Humans as Decision Makers

Problem change recognition	Too conservative in recognizing changes in problem conditions; delays too long in response to those changes	Refs. 5, 6
Situation diagnosis	Poor at making diagnosis of complex situations entailing complicated interpretations of configural cue patterns	Refs. 2, 6
Formulation and selection of action alternatives	Not sufficiently inventive and tends to adopt the first solution developed Forms hypotheses early, then tries to confirm rather than test them; does not consider enough hypotheses	Refs. 2, 6 Ref. 5
Identification and use of decision criteria	Finds it difficult to use more than one or two criteria at a time; tends to identify only those criteria favorable to selected action	Refs. 2, 6
Use of available information	Tends to use only concrete, high confidence facts and prefers to ignore ambiguous or partial data Asks for more data from sources of good-quality information Requests more evidence than is necessary for a decision	Refs. 2, 6 Refs. 5, 6 Ref. 5
	Poor at combining evidence to update probability estimates Gives undue weight to early events and is reluctant to change an erroneous commitment in light of new evidence	Ref. 5 Refs. 1, 5

Source: Boff and Lincoln. *Engineering Data Compendium: Human Perception and Performance*. 1988

Diagnosis challenges in NPPs



Operators faced serious challenges to diagnosis due to human limitations plus information limitations.

Sources of information limitations:

- **Plant Design:** Current sensors were not designed for accident monitoring
- **Guidance:** Operators lack guidance as to which information is most important in severe accidents
- **Guidance:** Operators lack guidance to turn observations into a diagnosis
- **Complexity/Dynamics:** Rapid scenario evolution, short response window

Cognitive challenges:

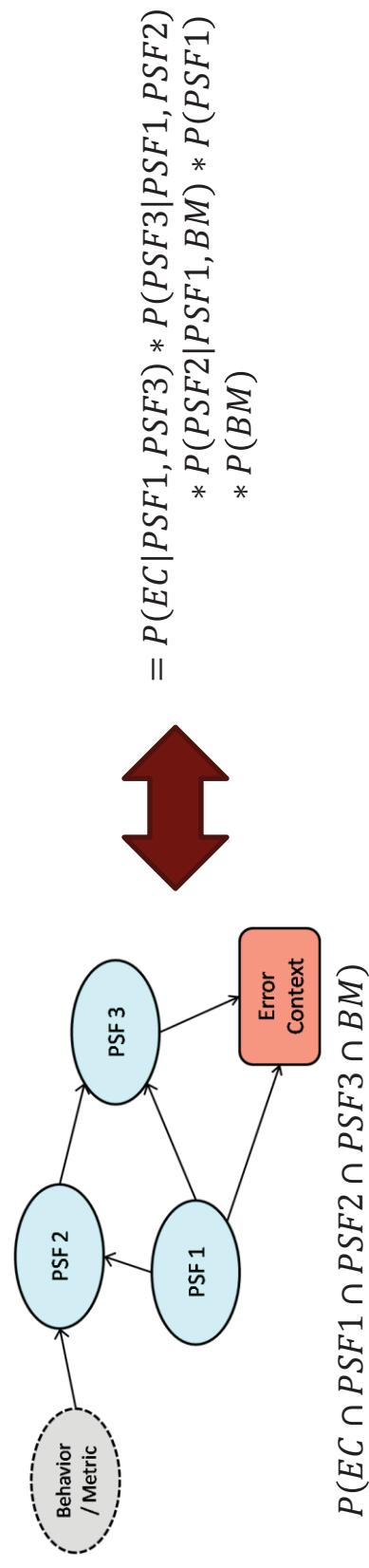
- **Understanding:** Developing a “big picture” from partial information
- **Filtering:** Deciding which information is relevant to the scenario
- **Prioritizing:** Deciding which information is worth expending limited resources

Supporting diagnosis

- Bayesian Networks (BNs) are used to support diagnosis activities in a range of industries
 - Medicine
 - HEPAR II: Diagnosis of liver disorders
 - CHILDE: Congenital heart disease diagnosis
 - MUNIN: Preliminary Diagnosis of neuromuscular diseases
 - SWAN: System for insulin adjustment for diabetics
 - PATHFINDER: Diagnosis of breast cancer
 - Business and Management
 - Finance-Fraud/Uncollectible debt collection
 - Engineering & Science
 - BOBLO: Expert system based for cattle blood group determination
 - Diagnosis of faults in waste water treatment process

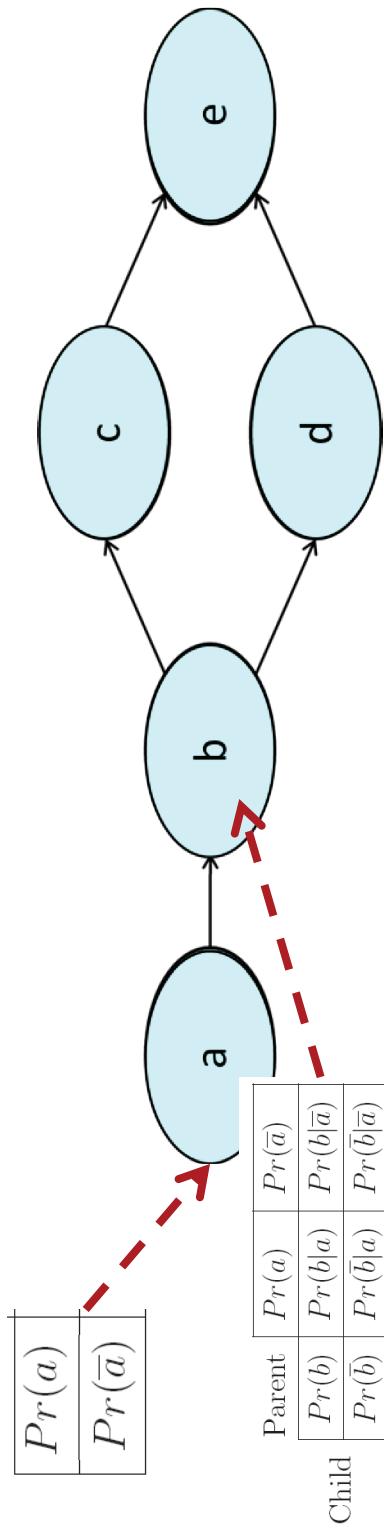
Tool: Bayesian Networks (BNS)

- A tool for:
 - Encoding a knowledge base
 - Performing reasoning with that knowledge base
- Benefits:
 - Credibility: Models built with info. & data from multiple sources
 - Flexibility: Simultaneously reasons forward and backward, about all variables in the model.
 - Simplicity: Compact representation of a large, high-dimensional problems
 - Handles uncertain information



Pieces of a BN

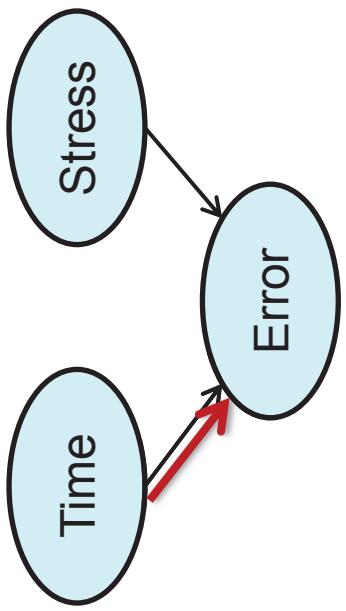
- Graphical model + Probability distribution
 - Relevant variables and their possible states
 - (In)dependency among variables
 - The simplified joint probability distribution of the system (based on conditional probabilities)



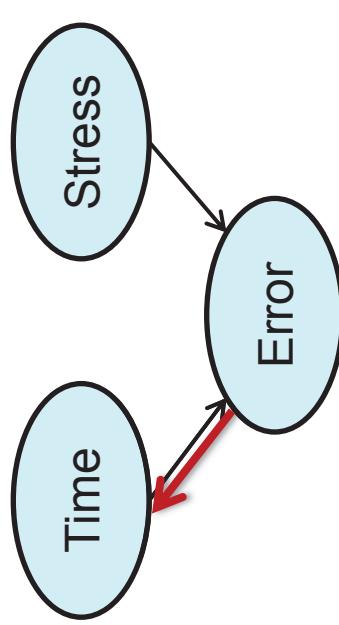
$$\begin{aligned} P(a, b, c, d, e) &= P(e|a, b, c, d,) * P(d|a, b, c,) * P(c|a, b,) * P(b|a) * P(a) \\ &= P(e|c, d) * P(d|b) * P(c|b) * P(b|a) * P(a) \end{aligned}$$

Types of reasoning/inference

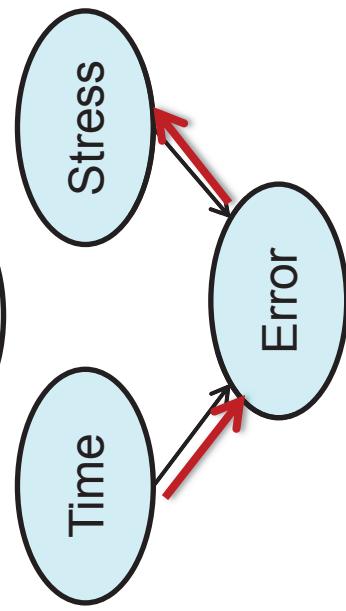
Causal:
(Forward, Inference)



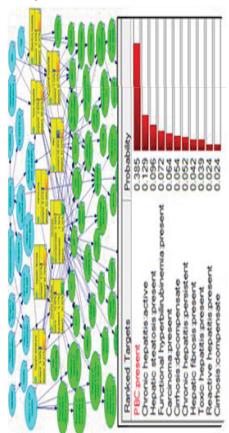
Evidential:
(Backward, Diagnosis)



Intercausal:



How diagnosis works



The generic knowledge base (BN) contains nodes and [prior] probabilities

- Components of the system,
- How possible defects manifest through symptoms, test results, error messages etc.

Observations:

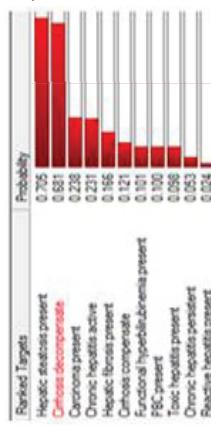
- Sex: male
- Irregular liver: present
- History of alcohol abuse: present
- Platelet count: 0-99

Users make observations about known symptoms or test results for a specific situation/person

Parent	$Pr(a)$	$Pr(\bar{a})$			
Child	$Pr(b)$	$Pr(b a)$	$Pr(\bar{b} a)$	$Pr(b \bar{a})$	$Pr(\bar{b} \bar{a})$
$Pr(\bar{b})$	$Pr(\bar{b})$	$Pr(\bar{b} a)$	$Pr(b \bar{a})$	$Pr(\bar{b} \bar{a})$	$Pr(b \bar{a})$

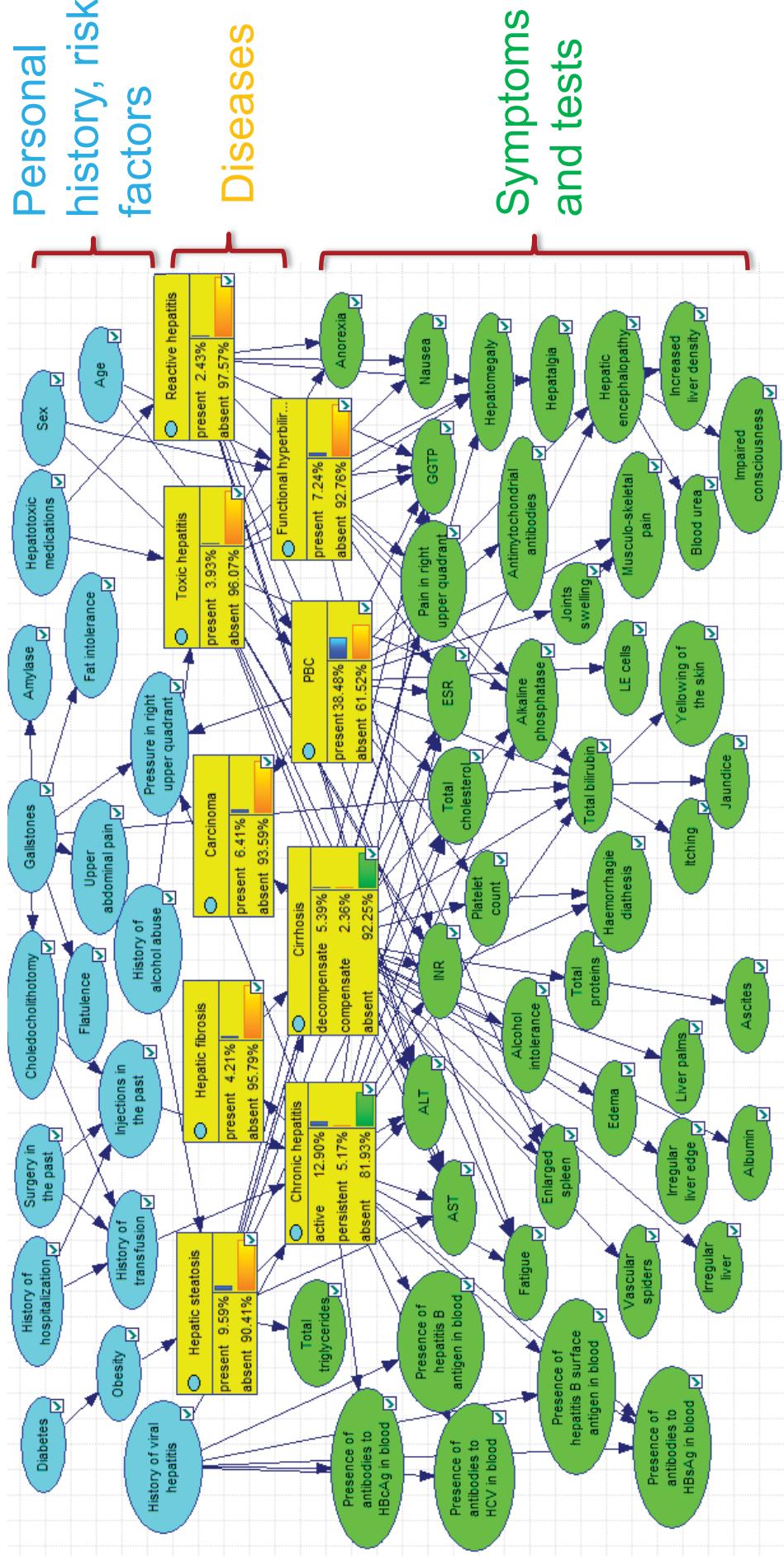
$$P(X_1, X_2, \dots, X_n) = \prod_i P(X_i | \text{Par}_G(X_i))$$

Observations are propagated (forward and backward) through the network to provide posterior probability of every node



Posterior probability can be used for reasoning (e.g., ranking diseases, selecting tests, calculating value of information for tests)

BN for diagnosis of liver disorders (HEPAR II)

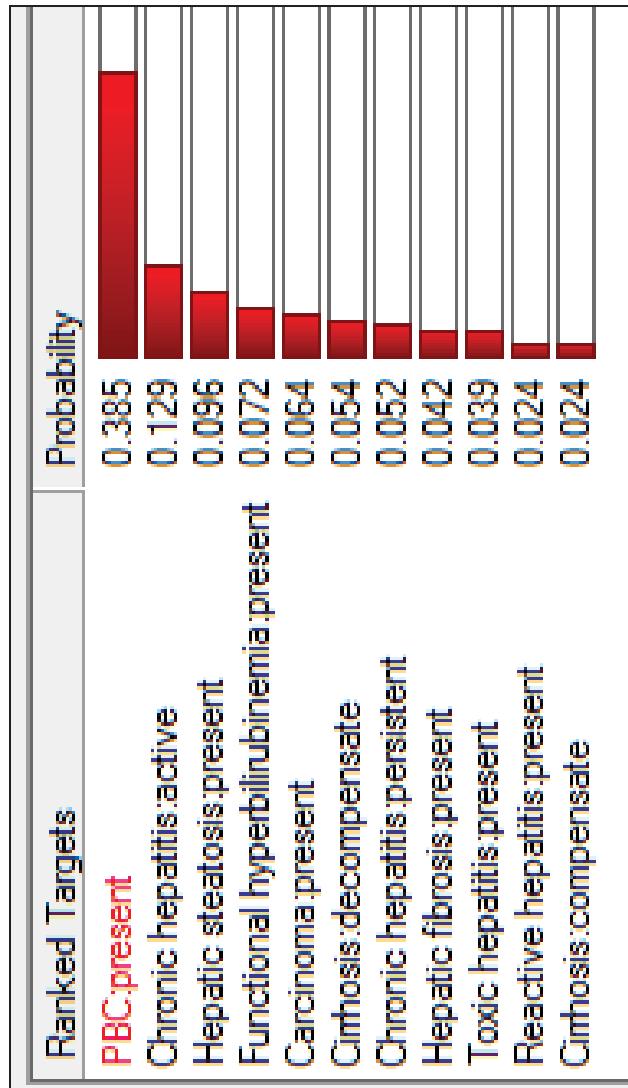


Source: Onisko 2003

Implemented in GeNIE: <http://genie.sis.pitt.edu/>

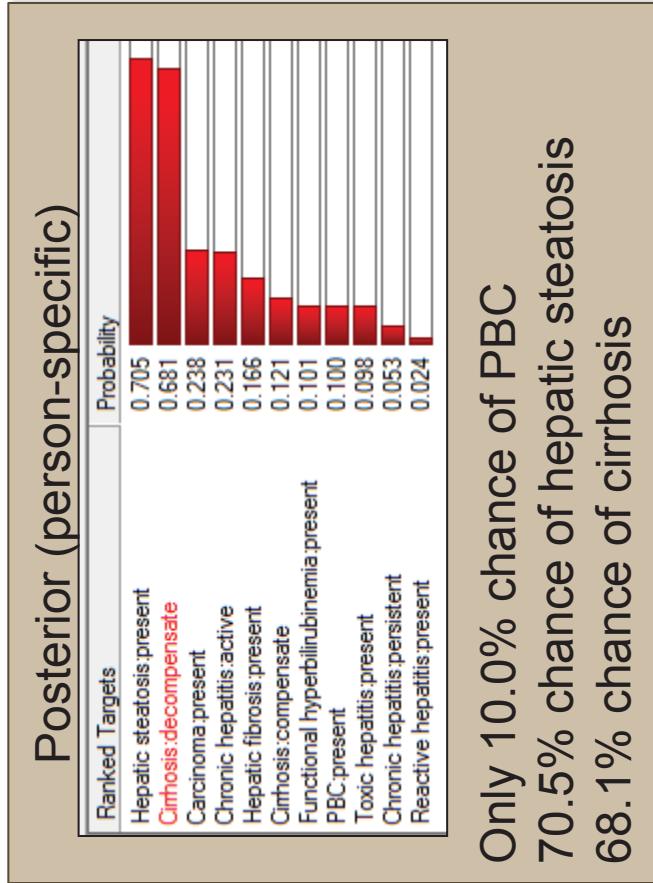
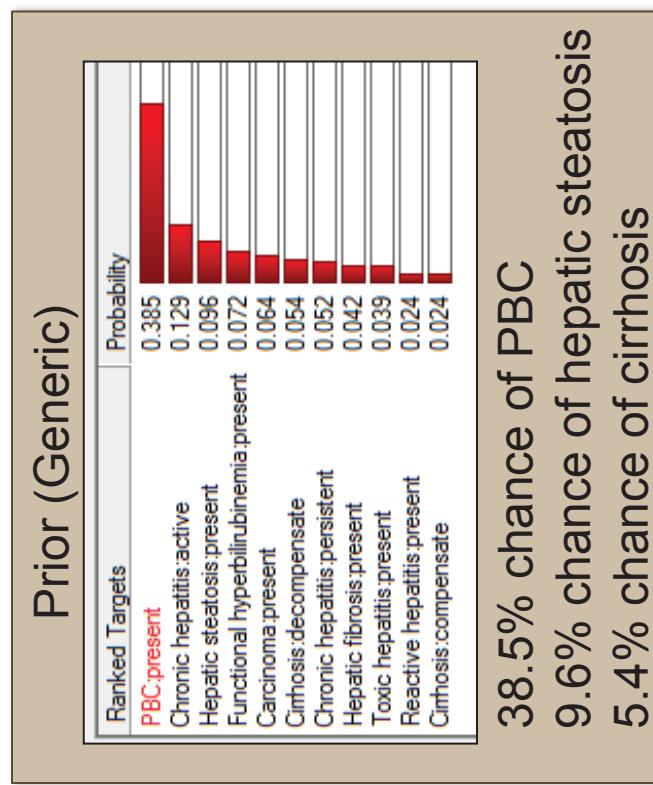
Probability of liver disorders (prior)

- Probability of having each disease
- This is the *prior* – for a generic member of the population
- Calculated in BN by law of total probability and subsequent marginalization



Prob. of liver disorders (posterior)

- Observations (4, of the ~70 possible):
- Sex: male
 - Irregular liver: present
 - History of alcohol abuse: present
 - Platelet count: 0-99



Only 10.0% chance of PBC
70.5% chance of hepatic steatosis
68.1% chance of cirrhosis

38.5% chance of PBC
9.6% chance of hepatic steatosis
5.4% chance of cirrhosis

A few key observations dramatically change disease likelihood

Diagnostic value of additional tests

For hepatic steatosis

Ranked Observations	Diagnostic Value
Total triglycerides	0.091
Irregular liver edge	0.047
INR	0.044
Vascular spiders	0.032
Enlarged spleen	0.025
Albumin	0.024
Liver palms	0.023
AST	0.019
Total cholesterol	0.018
GGTP	0.016
Total bilirubin	0.014
ALT	0.012
Alkaline phosphatase	0.012
Antimyochondrial antibodies	0.008
ESR	0.008
Edema	0.008
Presence of hepatitis B surface antigen...	0.007

Suggested tests/symptom checks:
triglyceride count, INR, liver edge

For cirrhosis (decompensate)

Ranked Observations	Diagnostic Value
Irregular liver edge	0.143
Enlarged spleen	0.077
Liver palms	0.070
Vascular spiders	0.066
Edema	0.057
Albumin	0.044
INR	0.038
Total bilirubin	0.033
Total triglycerides	0.015
Antimyochondrial antibodies	0.014
Alkaline phosphatase	0.013
Yellowing of the skin	0.010
Hepatic encephalopathy	0.006
GGTP	0.004
Total proteins	0.004
AST	0.004

Suggested tests/symptom checks:
liver edge, enlarged spleen, liver palms

Notice: different tests / symptoms provide greater diagnostic power for different diseases (and some provide very little value for either disease)

Diagnostic value calculations

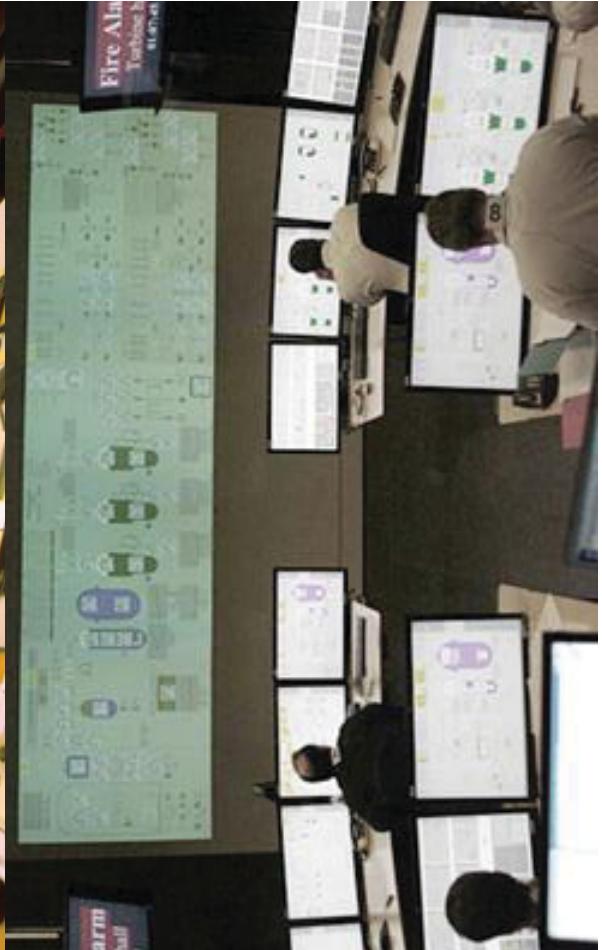


- Feature of GeNle package (other packages may contain similar features).
- Multiple algorithms included in GeNle – See Jagt 2002.
 - Based on expected gain in cross-entropy between the test and the disease/fault
 - Conceptually: $\text{Entropy}(\text{fault}_n) = P(\text{Fault}_n | \text{Test}_i)$
 - Multiple-cases: Based on differential diagnosis using joint probability (generated from copulas) or marginal probability

Outline

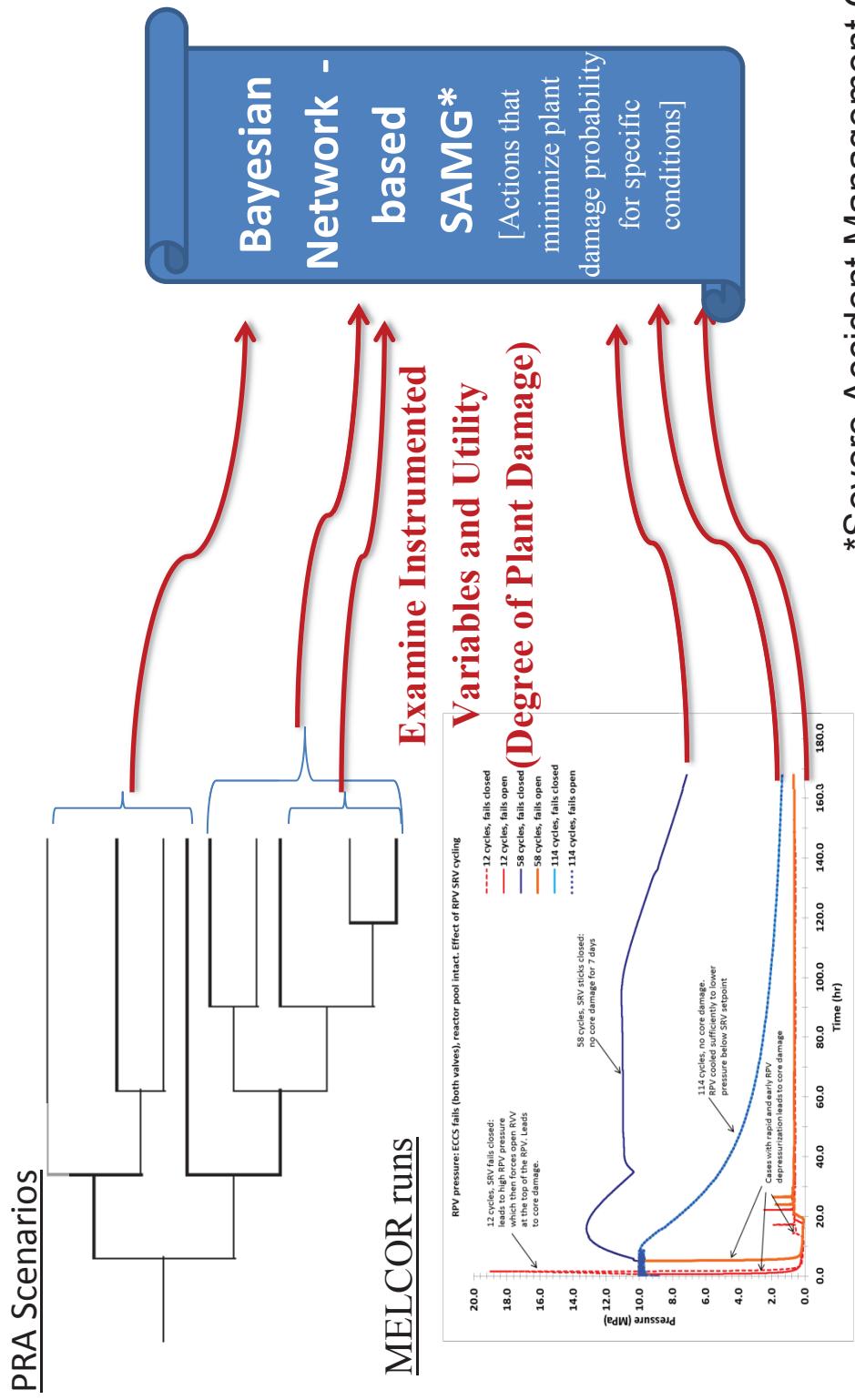
- Background
 - Why fix procedures?
(optional)
 - “Smart procedures”
research

Photo Credits:
Top: Tennessee Valley Authority
Bottom: Halden Reactor Project



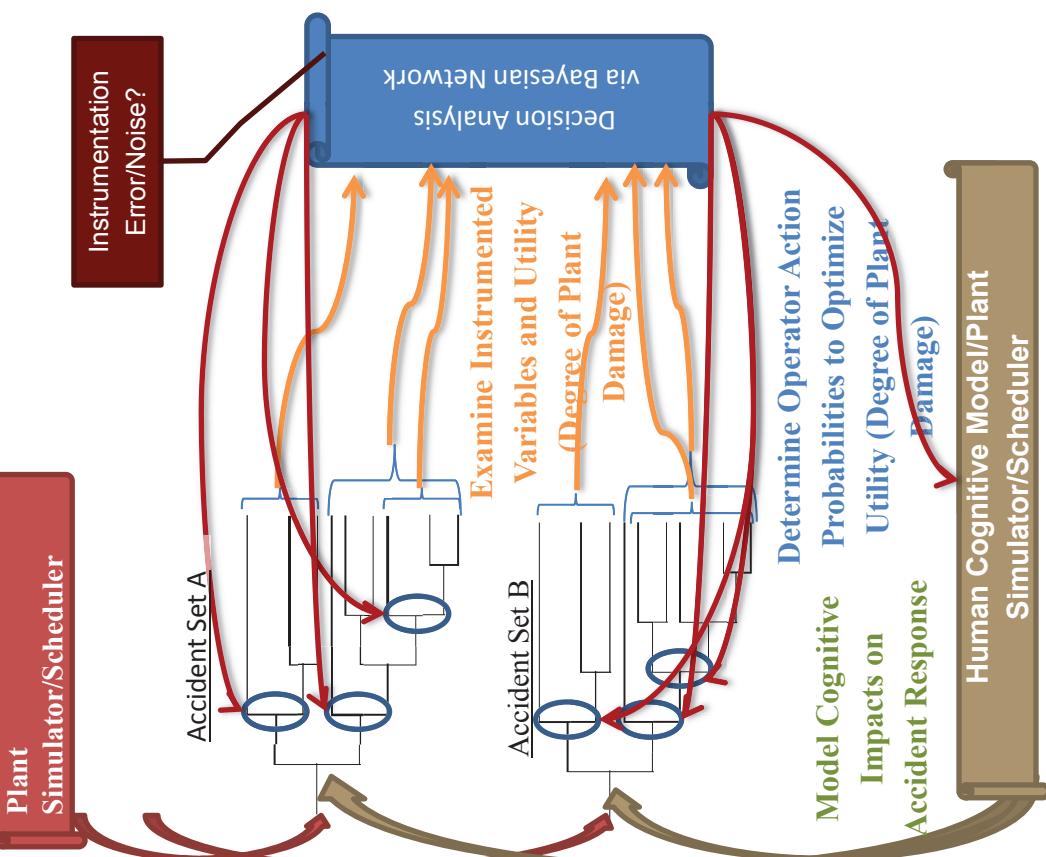
Smart SAMGs in a nutshell

- Build a knowledge base from PRA output & MELCOR runs
- Use it for real-time reasoning (or simulating an operator)



*Severe Accident Management Guidelines

Extension to simulation-based PRA



- Smart SAMG (built after first set of PRA/MELCOR runs) serves as a surrogate procedure for predicting human actions in subsequent PRA runs.

Theories underlying this work



Sandia
National
Labs

1. BN-based decision support systems (DSS) can be built to support diagnosis of severe accidents in NPPs.
 - Rationale: Direct analogue to work in other industries
 - FY13 progress: Built proof of concept model to demonstrate this
2. These decision-support systems can also function as surrogate humans (*following procedures*).
 - Rationale: BNs are an expert system. The whole point of expert systems is to emulate human experts.
 - Subject of future work (FY14?) – Must implement sampling approaches to tie into ADAPT/IDAC.

Assumptions



- Operators act rationally and choose indicators that maximize diagnosis value for an expected accident.
 - Rationale: Trained operators will choose high-impact information (we can probably link this to some references from psychology).
- **Operators are not all-knowing**
- Different accident sequences present different patterns of key indicators.
- ...and MELCOR simulations can be used to predict these key indicators, for a given plant configuration.
- **...and operators cannot be presented with perfect information in real time.**

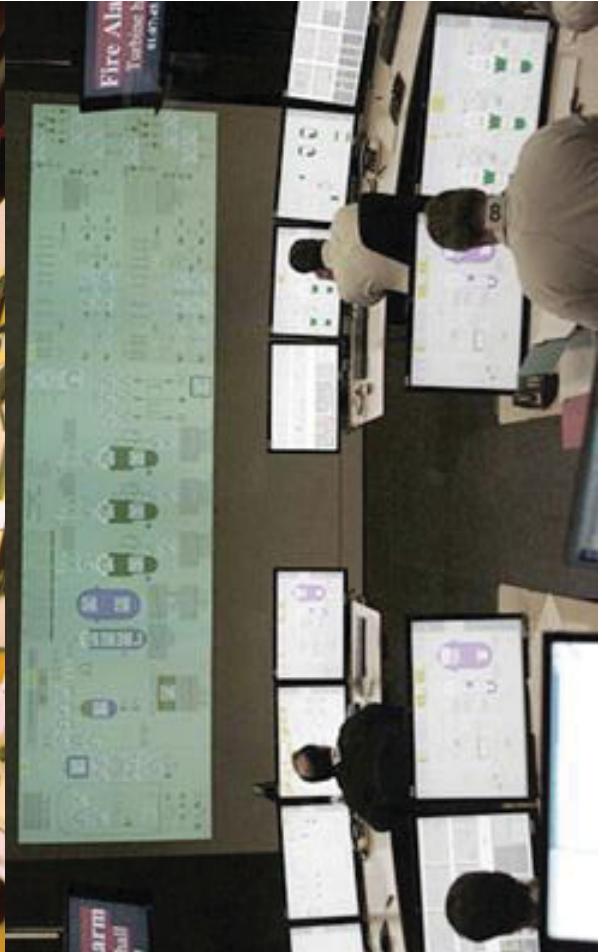
Approach

- Follow the medical model to help operators predict “diseases” in the plant and plant “tests”, given “symptoms”.
 - Just like doctors...operators do not have the capability to run every test and check every parameter.
 - Furthermore, some test have more value than others.
- Use robust information to quantify the prior model
 - Use MELCOR to simulate a large spectrum of possible accidents, for known plant conditions
 - Use PRA information to build probability of plant conditions
- Use knowledge base (Bayesian Network) for reasoning about plant conditions based on partial knowledge – either during accidents or for simulation

Outline

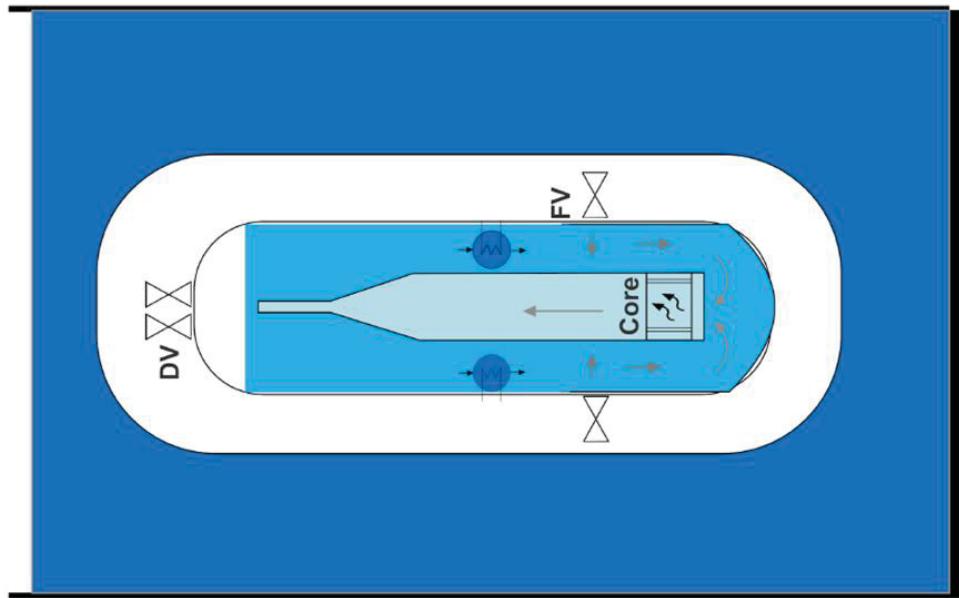
- Background
 - Why fix procedures?
(optional)
 - The prototype model

Photo Credits:
Top: Tennessee Valley Authority
Bottom: Halden Reactor Project



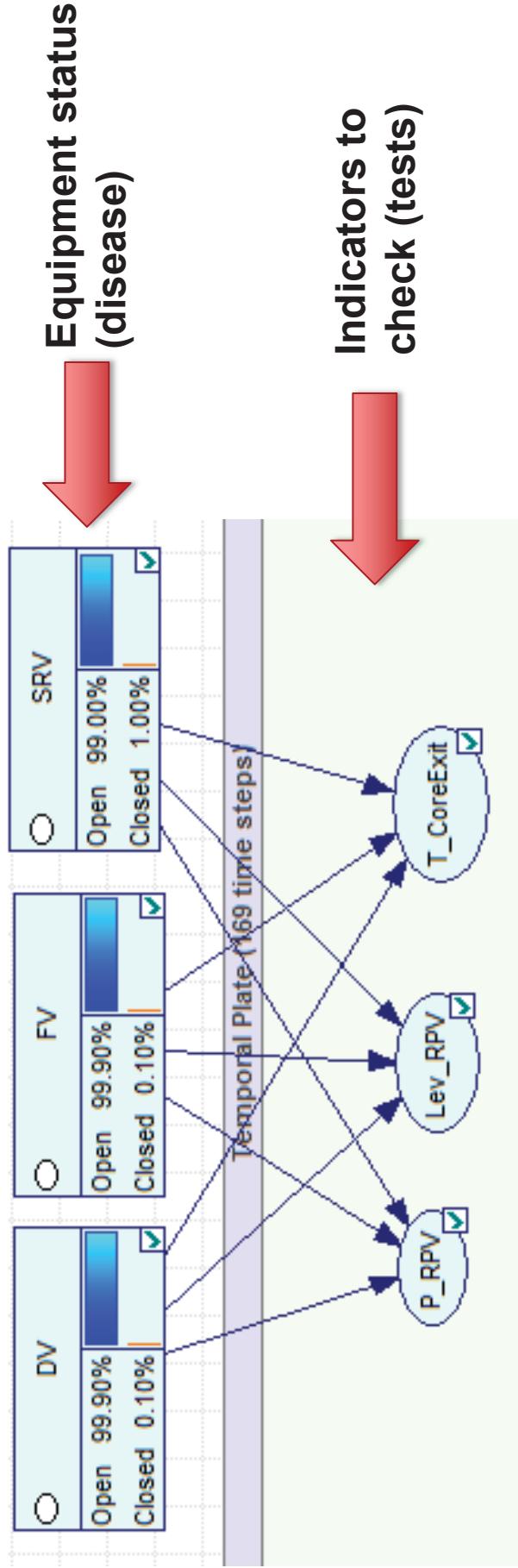
Example system

- Generic SMR design (one unit)
 - 120 MW_{th} Reactor
 - Submerged in a pool
- Emergency Core Cooling System (ECCS) is composed of:
 - Depressurization Valves (DVs)
 - Feed Valves (FVs)
- Passive flow system, no safety related pumps
- Goal: diagnose loss of ECCS by assessing status of FV and DV.

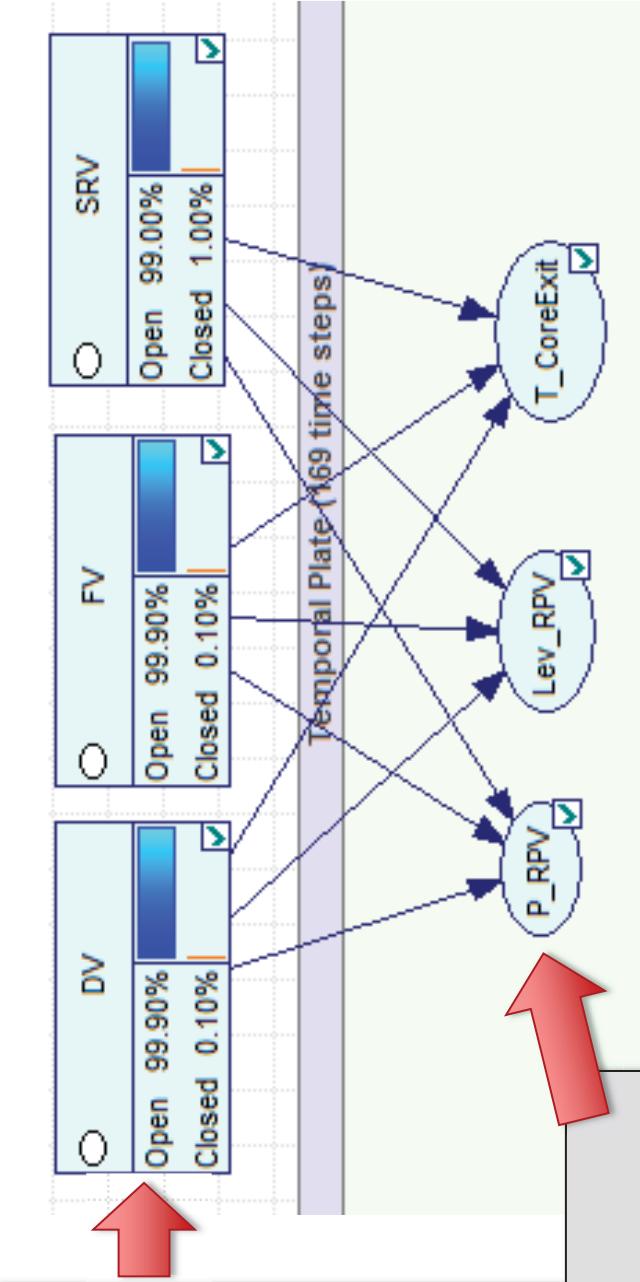
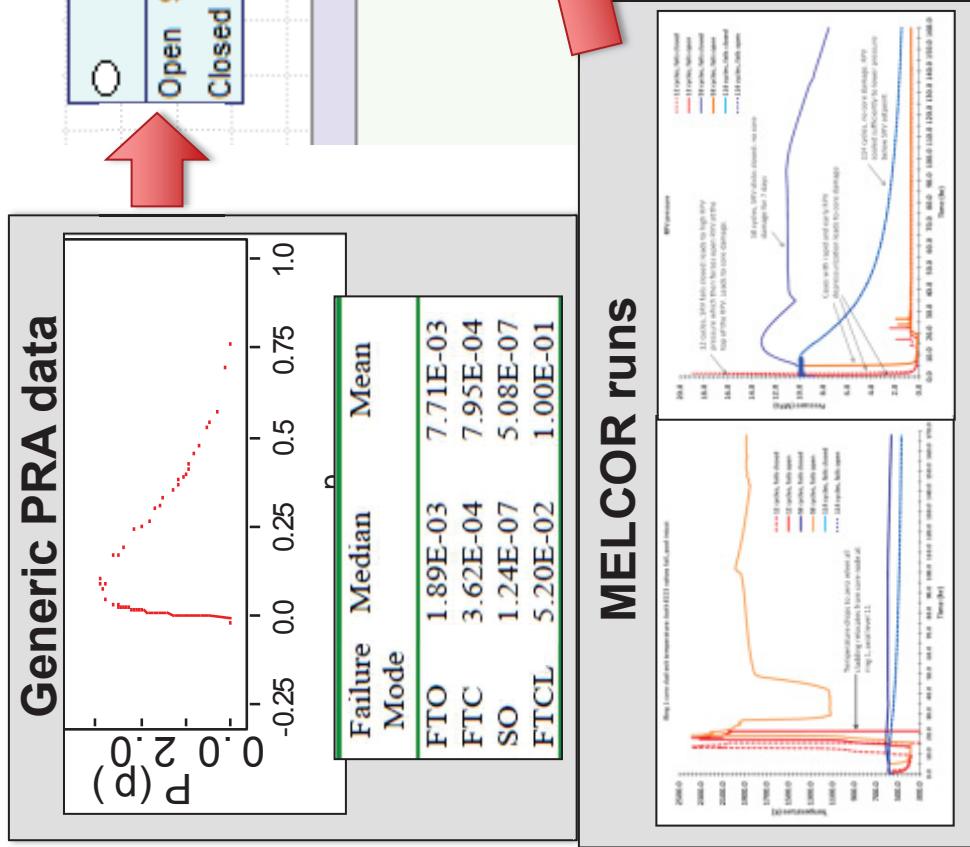




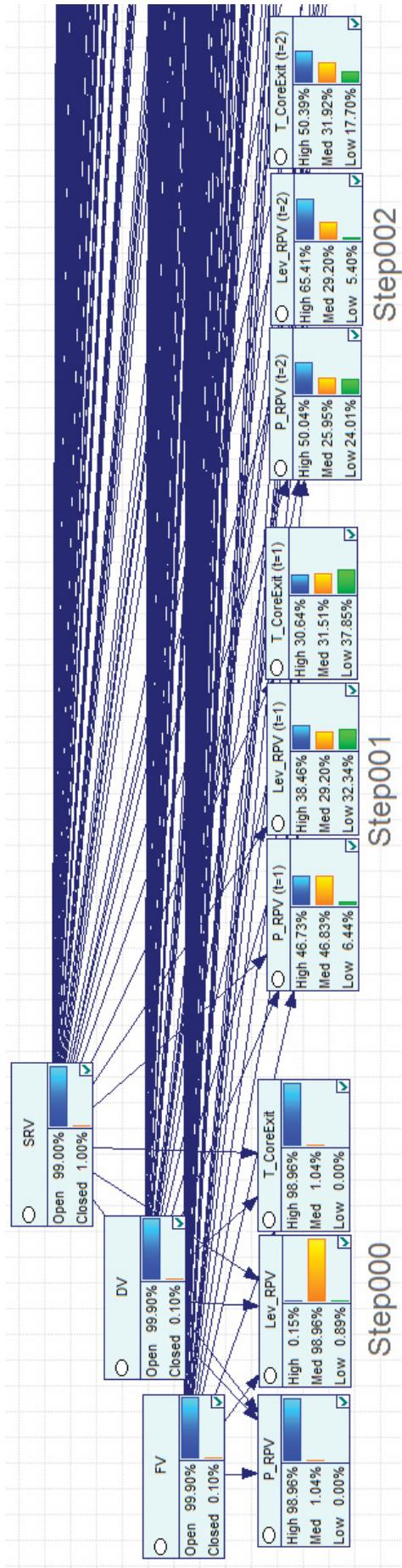
Proof-of-concept structure(compact)



Quantifying the prior



“Unrolled” dynamic model

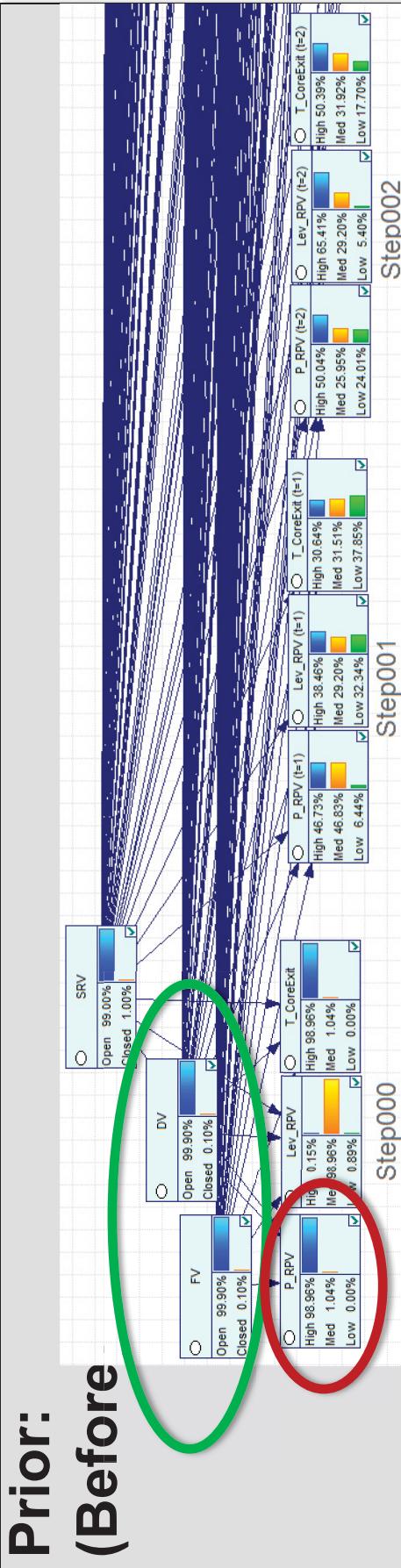


- 169 time steps (hrs, 0:168)
- Data as of May 13 MELCOR runs
 - These data runs provided reactor parameters for 57 cases with FV FTO. (FV closed, DV open). (Model needs to be updated using full set of runs, which are pending)
 - SRV node is included in model, but not yet included in quantification

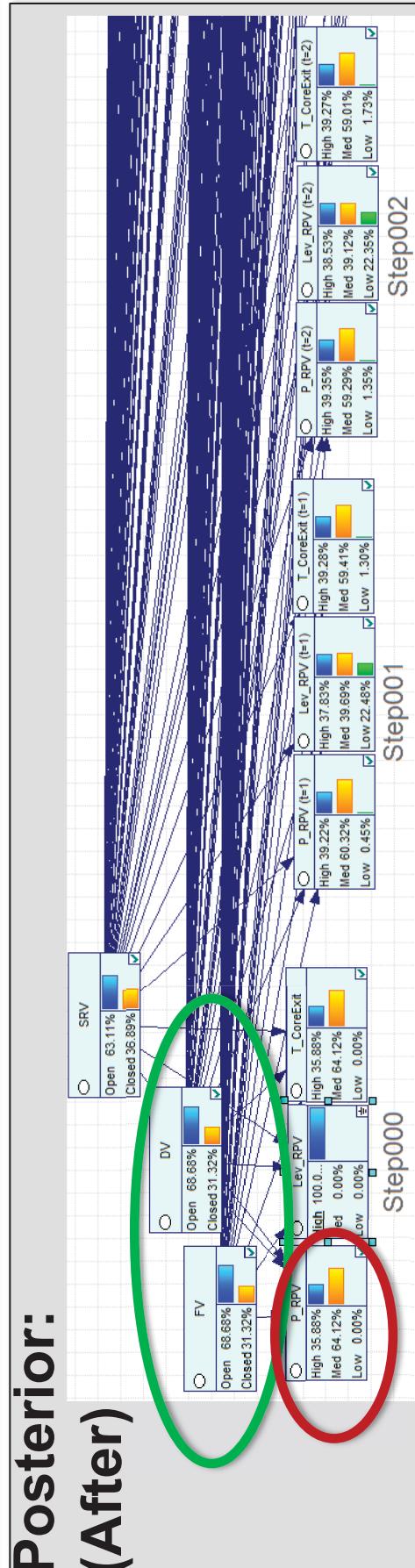
Backward reasoning (diagnosis)

- Changing about RPV level (to “high”) changes belief about status of FV and DV (....and also the other parameters)

Prior:
(Before)

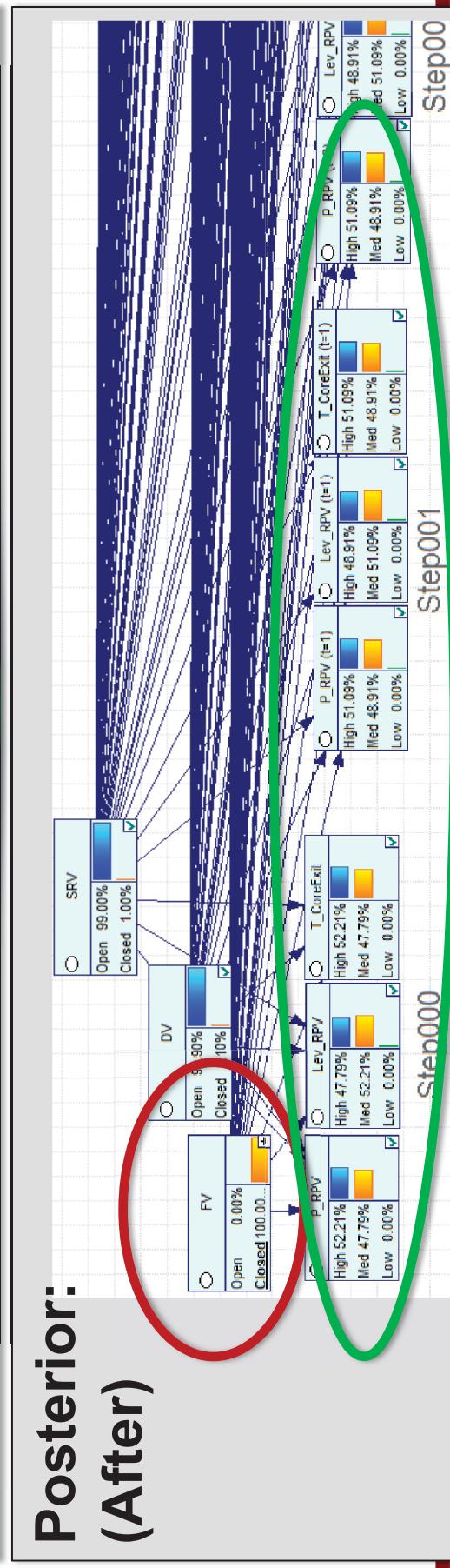
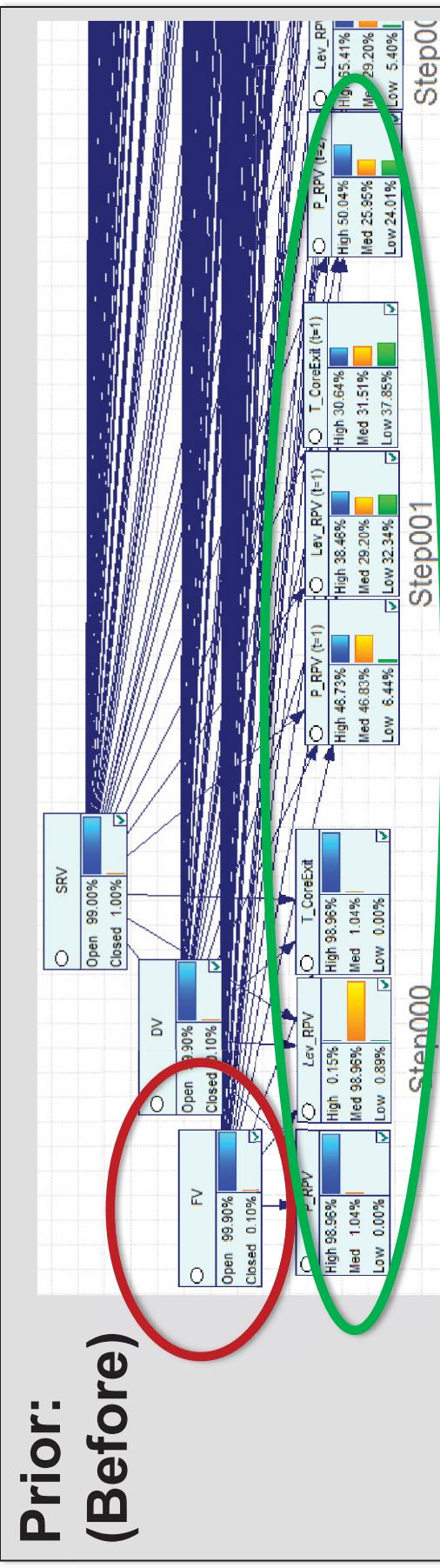


Posterior:
(After)



Forward reasoning

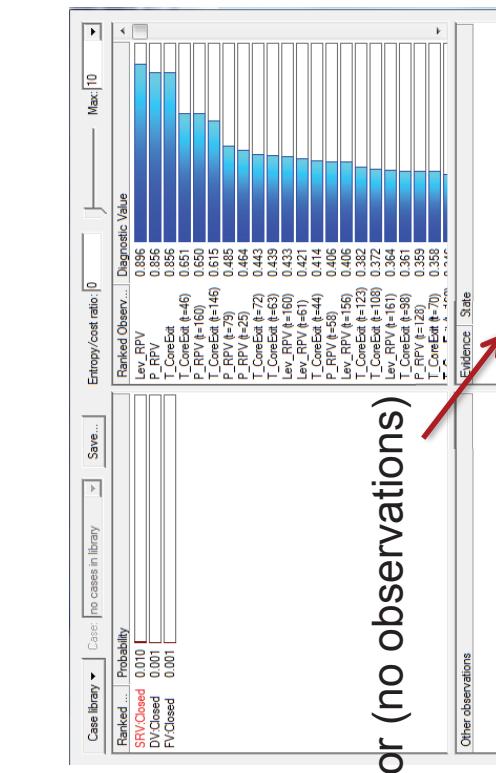
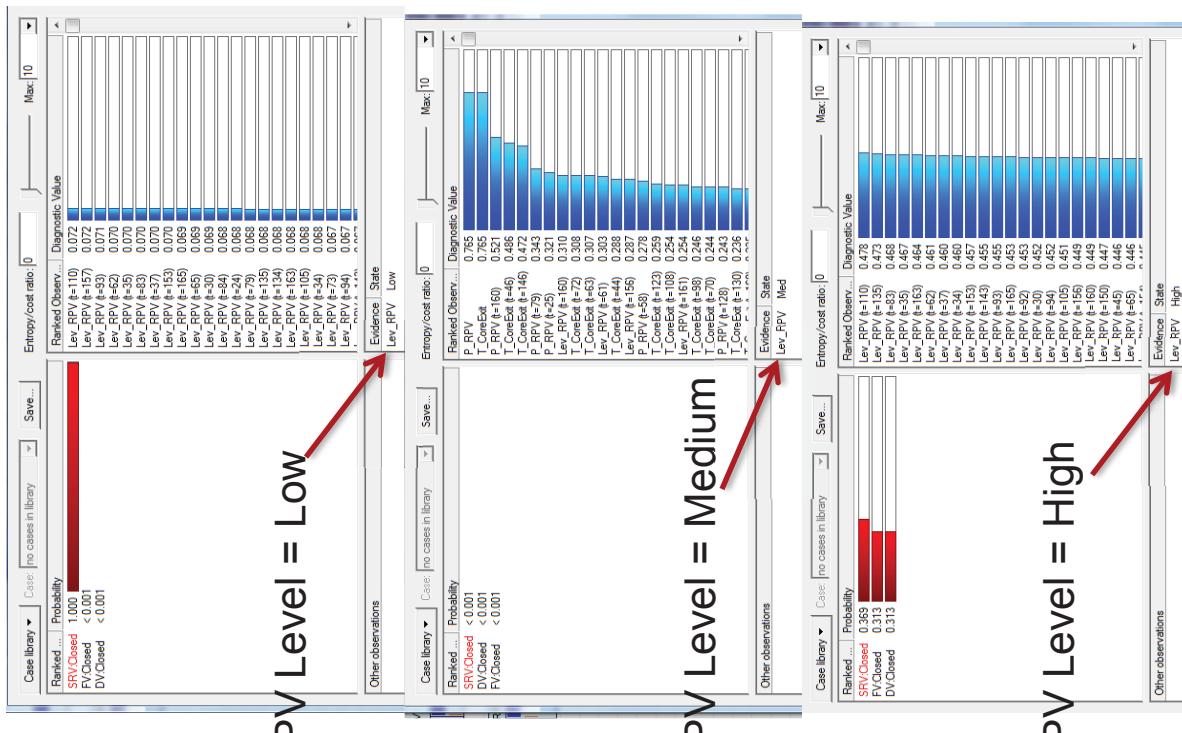
- Changing belief about FV (to FV=Closed) changes expectations about the parameters



Diagnosis view of model on previous slide

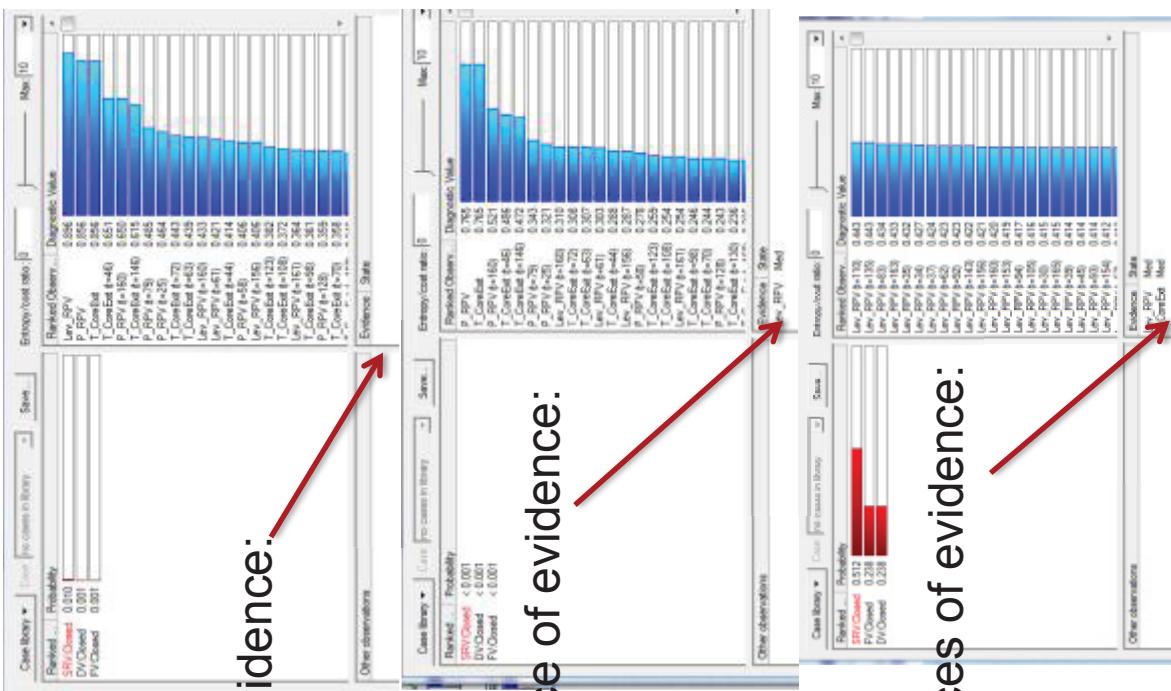


- Notice that beliefs about the status of the 3 valves (red bars) are updated after a single observations (“evidence” in bottom right corner) Likewise, diagnostic value of other observations is updated (blue bars).
- (Numbers are for example only, based on a non-representative set of Melcor runs, will be updated when comprehensive runs are complete.)



Diagnosis view (2)

- Additional evidence (bottom right box in each figure) will continue to update beliefs about the valve status and about diagnostic value of other observations.



Notice: In box 3, P_RPV is no longer among the top-ranked indicators. In fact, all of the best indicators are RPV Level (at different times). This shows operators or analysts that the critical information to seek is RPV Level.

Summary: Smart procedures

- Impact: Revolutionary way of thinking about procedures (not just SAMGs)
- New application for risk-information
- Benefits:
 - Dynamic updating of crew situational awareness
 - Guides operators to seek high-impact information
 - Improving the procedures can reduce human errors, workload.
- Why it will work:
 - Bayesian Networks are the reasoning framework underlying reasoning systems for medical diagnosis, fault diagnosis, etc.

References

- BNs
 - Onisko, A. (2003). *Probabilistic Causal Models in Medicine: Application to Diagnosis of Liver Disorders*. Ph.D. Dissertation, Institute of Biocybernetics and Biomedical Engineering, Polish Academy of Science.
- Human Performance
 - Chang, Y. H. J. & Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: Part 3: IDAC operator response model *Reliability Engineering and System Safety*, 92, 1041-1060 .
 - Boff and Lincoln (1988). *Engineering Data Compendium: Human Perception and Performance*.
- Smart Procedures
 - Denman M. R.; M., G. K. & Wheeler, T. A. (2013). "Proof of Principle Framework for risk informed Severe Accident Management Guidelines." *Proceedings of Risk Management for Complex Socio-Technical Systems (RM4CSS)*, Washington DC.

Next steps (July 25th)

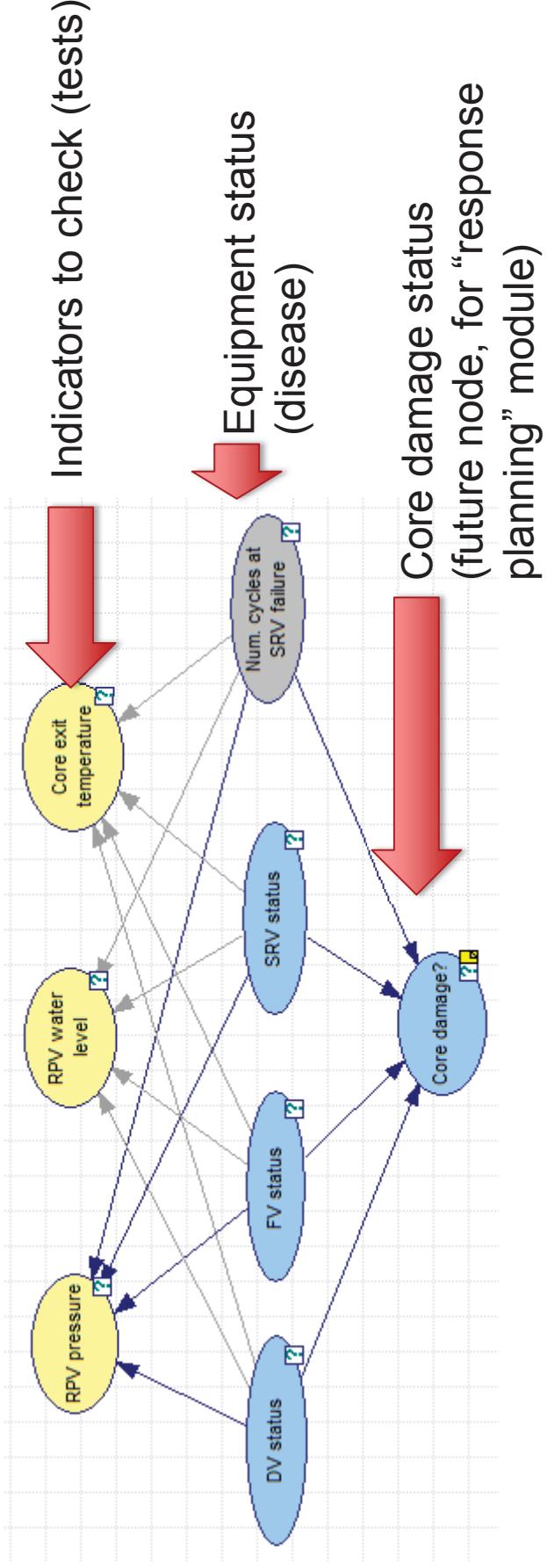


- Implement additional (non-failed) states for DV, FV,
- Determine how to implement dynamic SRV cycling
- Incorporate core damage node for risk-ranking
- Update with full set of Melcor runs

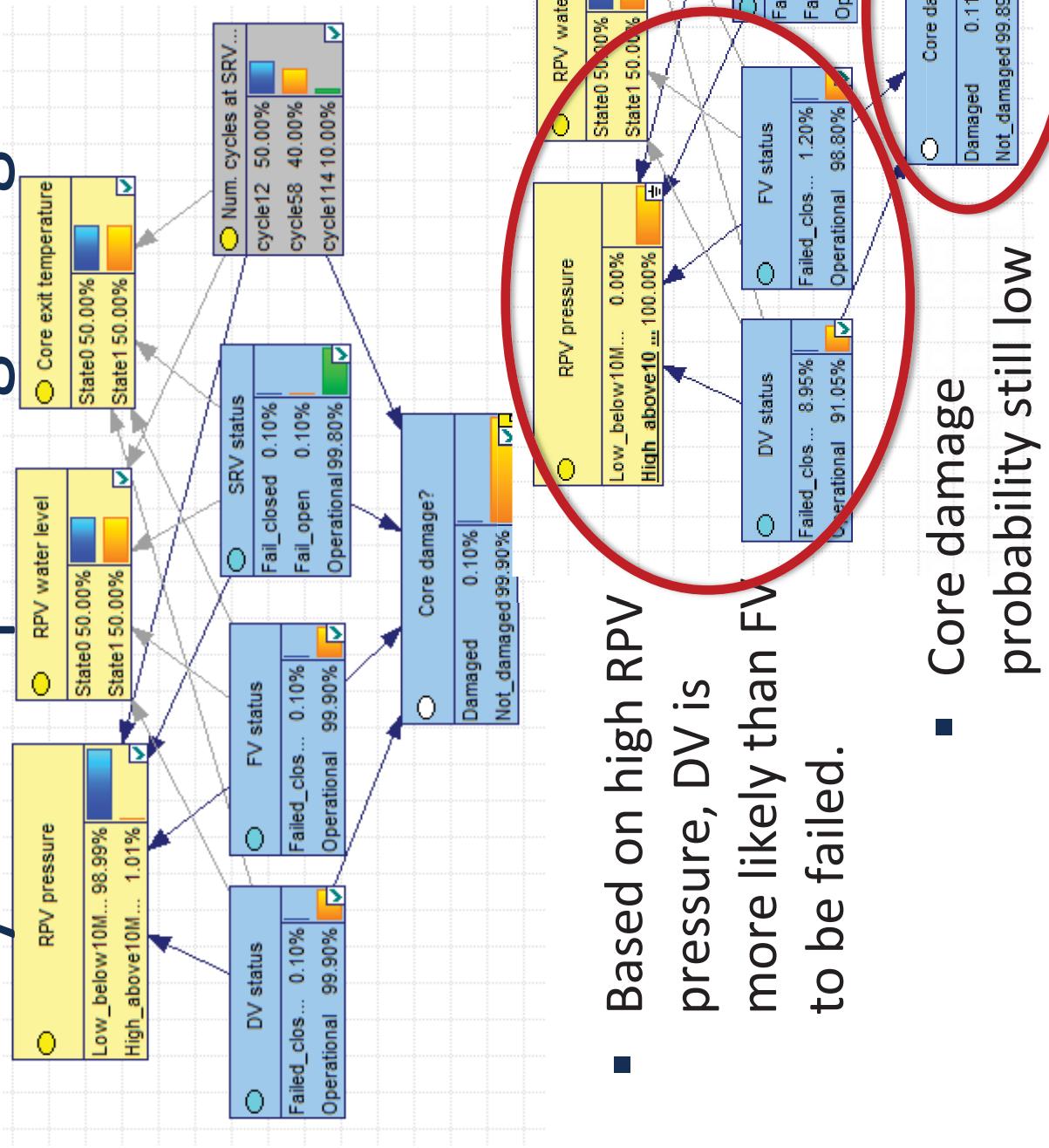
- Also need to generate documentation for the model, especially:
 - Algorithms for calculating diagnosis value
 - Valve states, assumptions, high-med-low bins
 - Details on scope of Melcor runs
 - Melcor results for different valve configurations for the 3 sensors.
- Longer term: implementation of action nodes, CVCS, etc.

Proof-of-concept SAMG structure

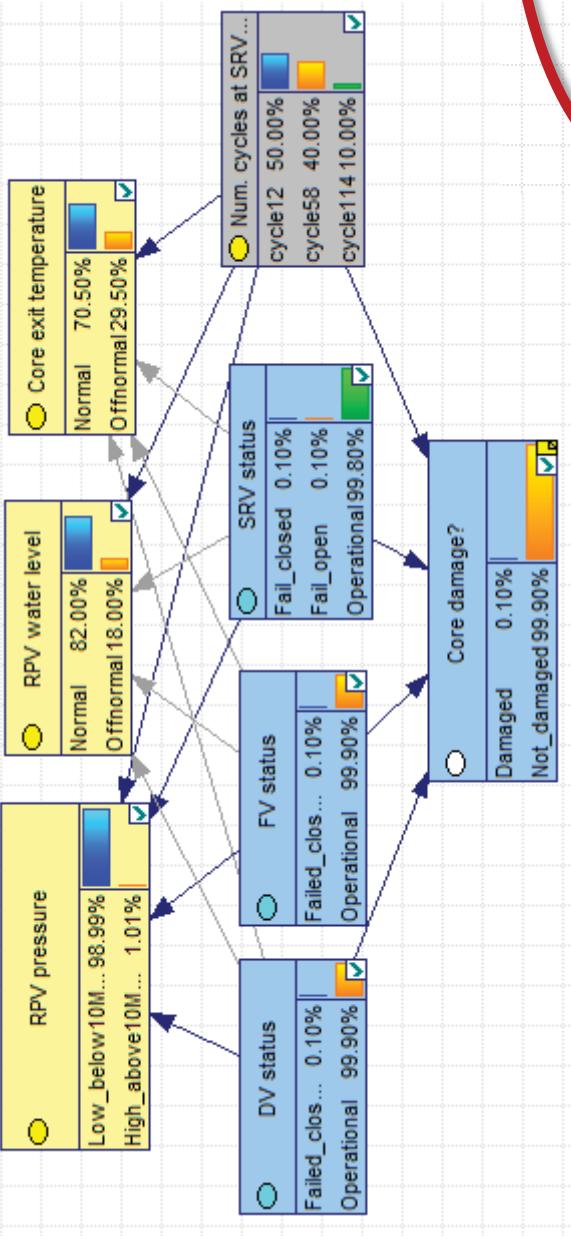
- (Simple, non-dynamic view)



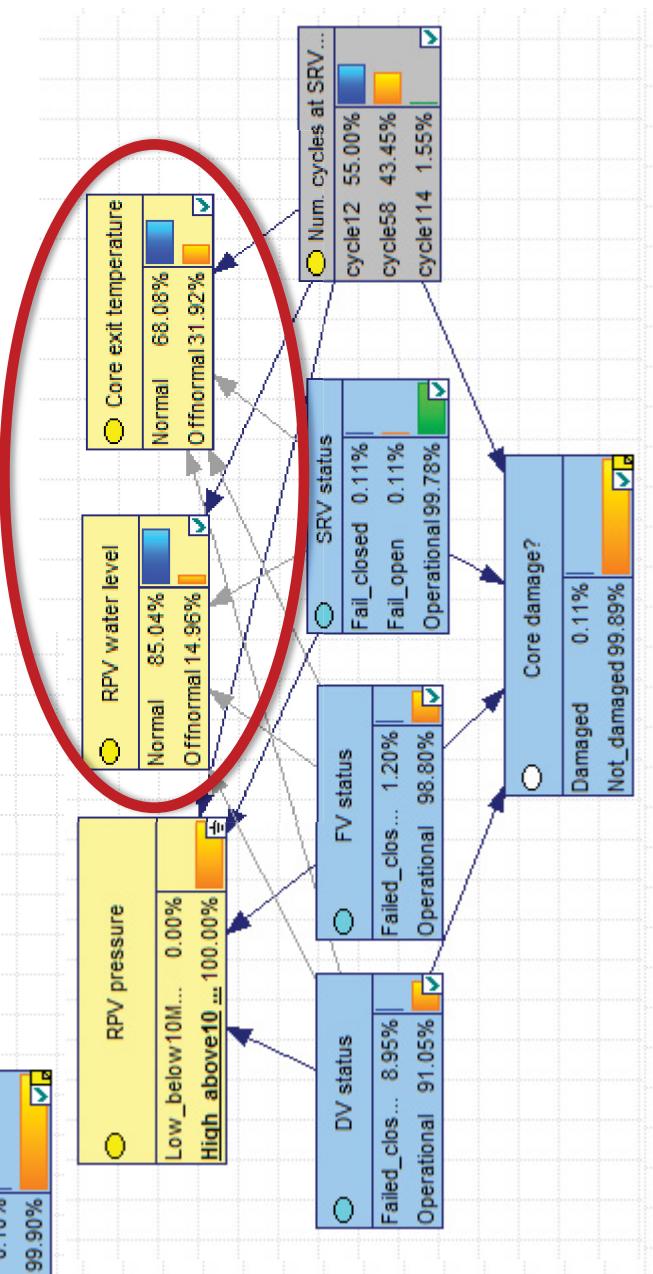
Bayesian updating: diagnosis



Bayesian updating: guidance



- When complete, BN will suggest:*
- Other indicators to check (to confirm DV problem)
 - Actions to take to resolve DV problem.



Dynamic PRA simulations at SNL

as of December 2012

Attribute	ADS-IDAC/MELCOR (AIM)	ADAPT-MELCOR for PWR	ADAPT-MELCOR for SMRs (DOE project)
Dynamic PRA code language	C++	Java/SQL	Java/SQL
Computer system	Windows PCs/ cluster	Linux cluster	Linux cluster
MELCOR model for demonstration problem	3-loop PWR: Surry SOARCA	3-loop PWR: Surry SOARCA 2 different simulations	1PWR: NuScale-type reactor
Size of MELCOR model for demonstration problem	Large: 86 COR cells, 144 volumes, 282 flow paths, 327 heat structures	Large: 86 COR cells, 144 volumes, 282 flow paths, 327 heat structures	Small: 38 COR cells, 70 volumes, 120 flow paths, 82 heat structures
Number of dynamic input variables	7	22/21 variables	12
MELCOR simulation success rate	55 – 60 % (?)*	55 – 60 %	80 – 90 %
Demonstration problem size	~648 branches	1372/4621 branches	576 branches
Max. number of successful branches	145 branches	776/2713 branches	468 branches
MELCOR simulation duration (time after accident initiation)	20 – 24 hours	96 hours (4 days)	168 hours (7 days)
CPU time for 1 complete branch	1.5 days	5-14 days	6-7 days
Total CPU time for simulation	24 weeks**	20/41 weeks	4 weeks

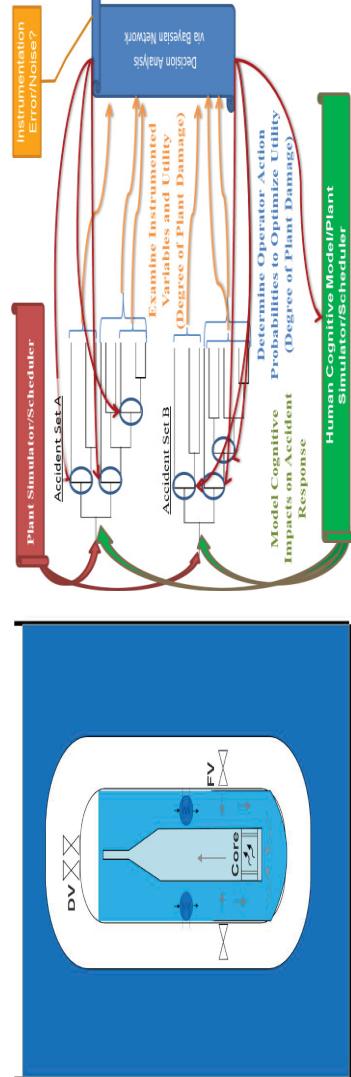
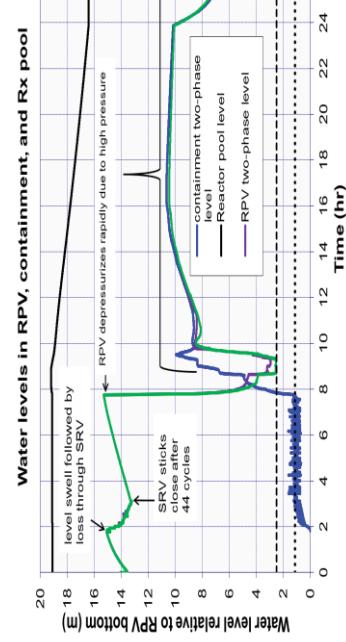
* Cannot directly calculate the success rate of the MELCOR Surry model with AIM project due to the serial execution of MELCOR simulations with the console version of ADS-IDAC. Roughly, the success rate would be about the same as the 50-80% success rate observed in the ADAPT-MELCOR simulation of the Surry SOARCA model (Doug Osborn's PhD topic). However, different accident sequences and boundary conditions were used in these two studies, and these have a strong influence on the success rate obtained from MELCOR.

** Estimated serial execution time if the simulation would have finished completely. MELCOR simulation errors prevented this.

Exceptional service in the national interest



Sandia
National
Labs



Risk-Informing Small Modular Reactor Safety Analysis

Dr. Matthew Denman, R&D S&E – Senior

Risk and Reliability

August 5-7, 2013 Beijing, China

Jeff Cardoni – MELCOR/ADAPT/IDAC guru
Dr. Katrina Groth – Bayan Network and Computer Support
Tim Wheeler – PRA and SMR safety

ACKNOWLEDGEMENTS

Purpose

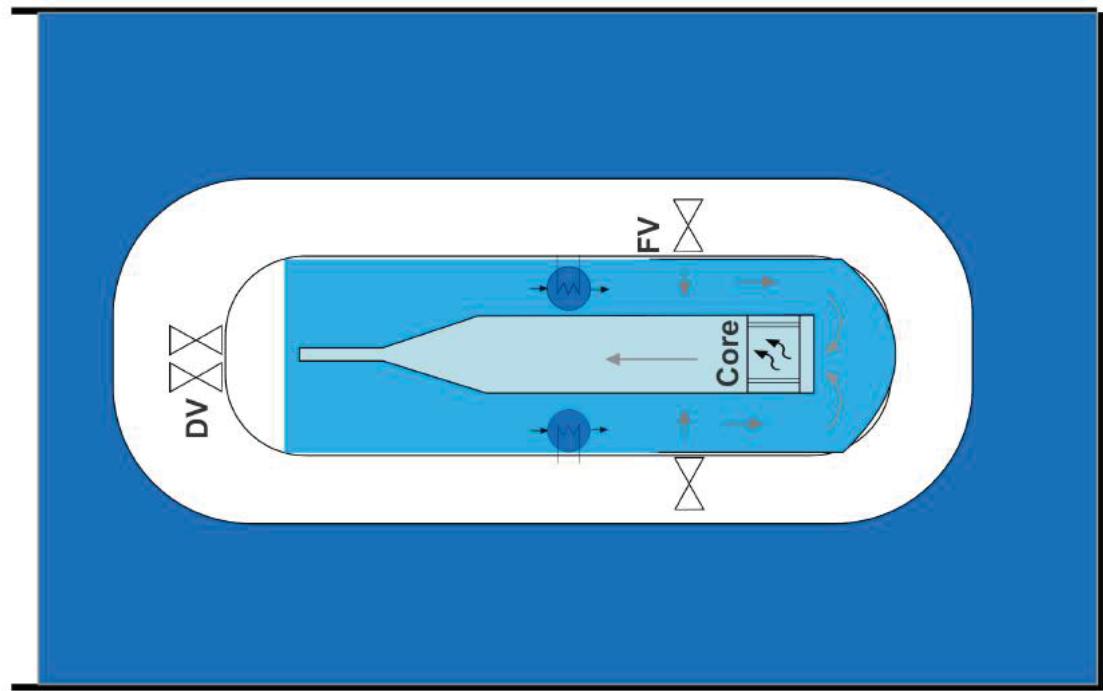
- Describe the promises of, and challenges of proving, the Small Modular Reactor (SMR) safety case.
- Describe the desire for risk-informed analysis when analyzing safety of SMRs
 - Emphasize that risk is more than just core damage frequency

Outline



- Overview of the generic SMR MELCOR Model currently used by SNL
- Desired regulatory changes
 - Safety benefits of SMRs
 - Challenges of proving that these benefits warrant change
 - New Risk Measures – Are existing OK and states really OK?
- Conclusions

Generic SMR MELCOR Model



Generic SMR Reactor

- Submerged in a pool sized to fit one reactor
 - 120 MW_{th} Reactor
 - Many one reactor pools can remain onsite
- Emergency Core Cooling System (ECCS) is composed of:
 - Depressurization Valves (DVs)
 - Feed Valves (FVs)
- Passive flow system, no safety related pumps

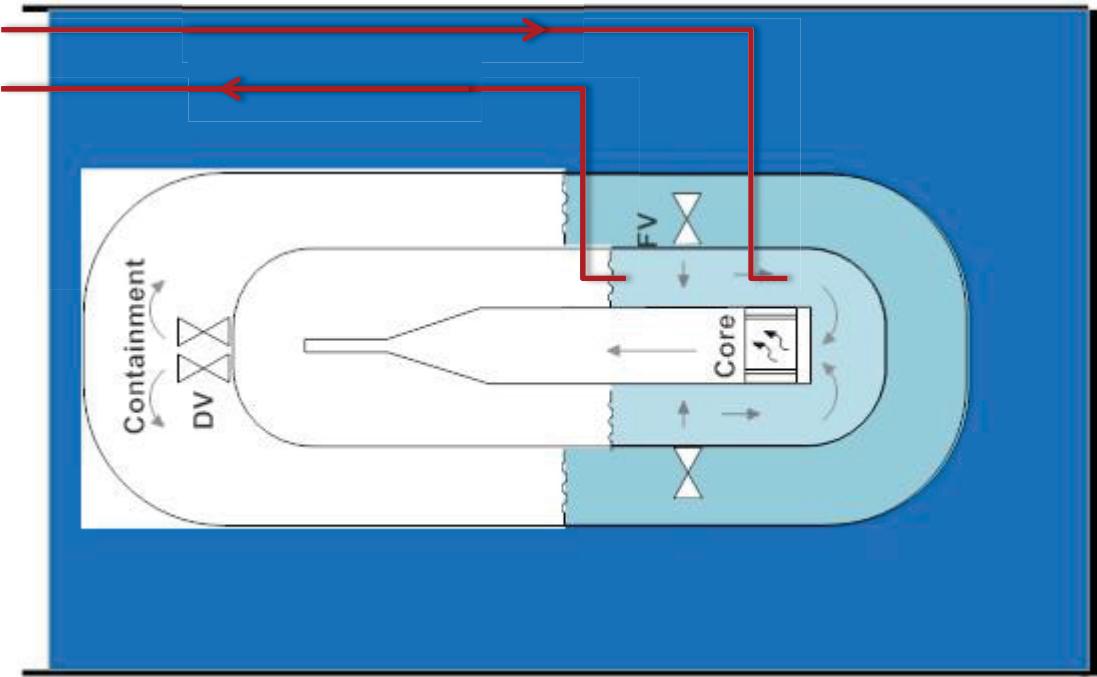
ECCS Operation

Non-Safety Grade Chemical Volume and Control System Interface



Sandia
National
Labs

CVCS system



Generic Submerged Reactor

- Operator can use Chemical Volume and Control System (CVCS) system to add water to the system
 - A small LOCA probability is assumed which can allow for containment bypass (unintended consequence).

Desired Regulatory Changes



Sandia
National
Labs

Rule Change

1. Smaller exclusion zone
 - Simpler emergency planning
 2. Reduced Staffing Requirements
 - Operational
 - Security
1. Smaller and Delayed Source Term
 - Smaller source term
 - Larger safety margins
 2. Passive Safety
 - Less need for operators
 - Less attractive to adversaries

Justification

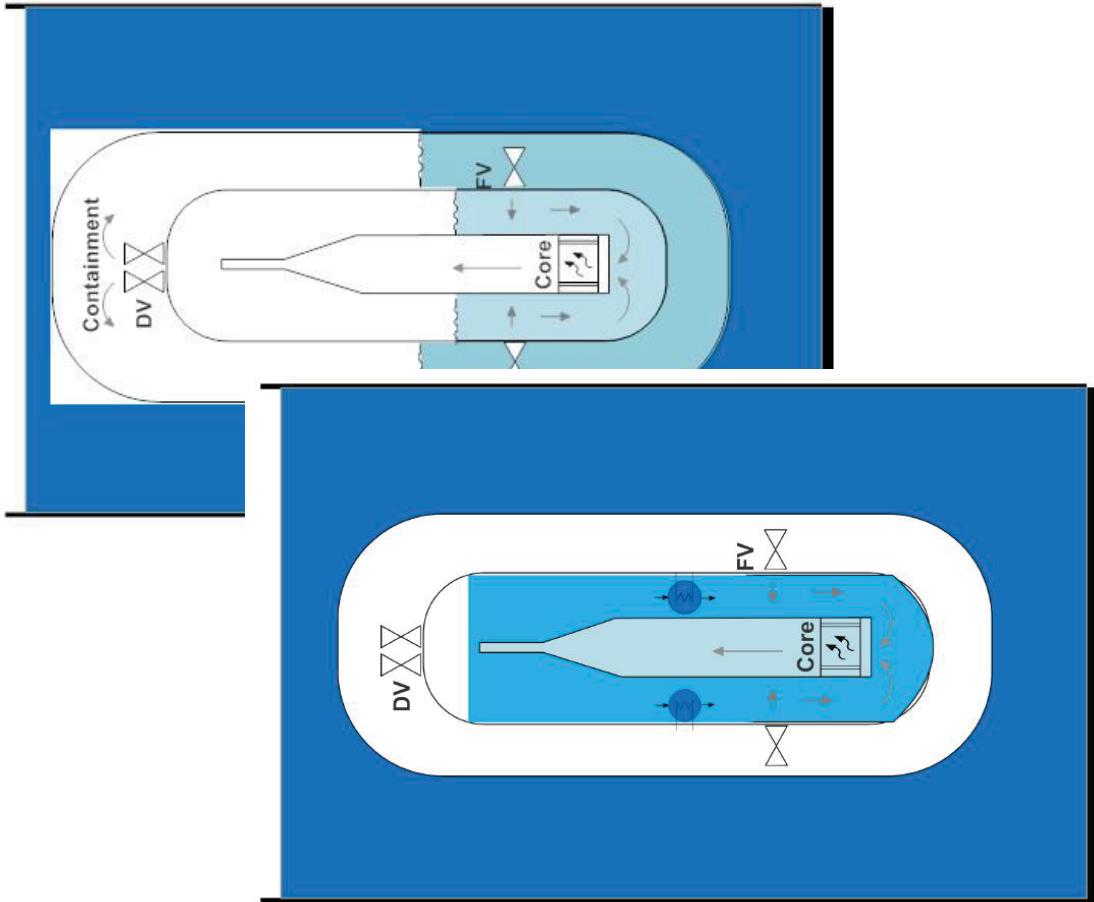
Risk-Adverse Regulatory Environment



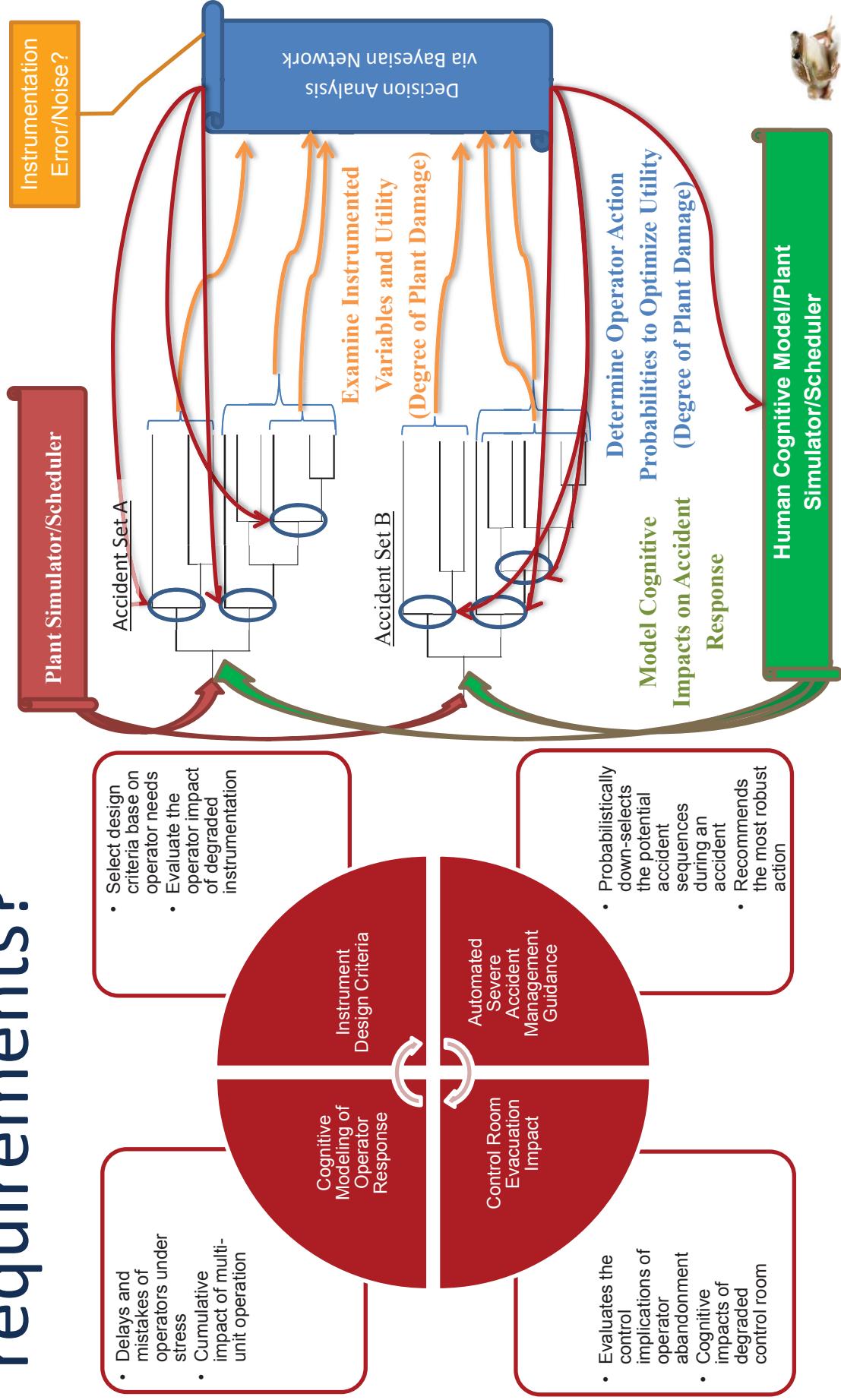
Sandia
National
Labs

Proposed rule changes prove challenging

- What is the cognitive load on an operator during an accident
 - Multi-tasking on multiple units?
 - Can human action unintentionally interfere with passive cooling?
- Containment bypass is always possible
 - Shared system vulnerabilities
 - Can multiple units can increase the site source term

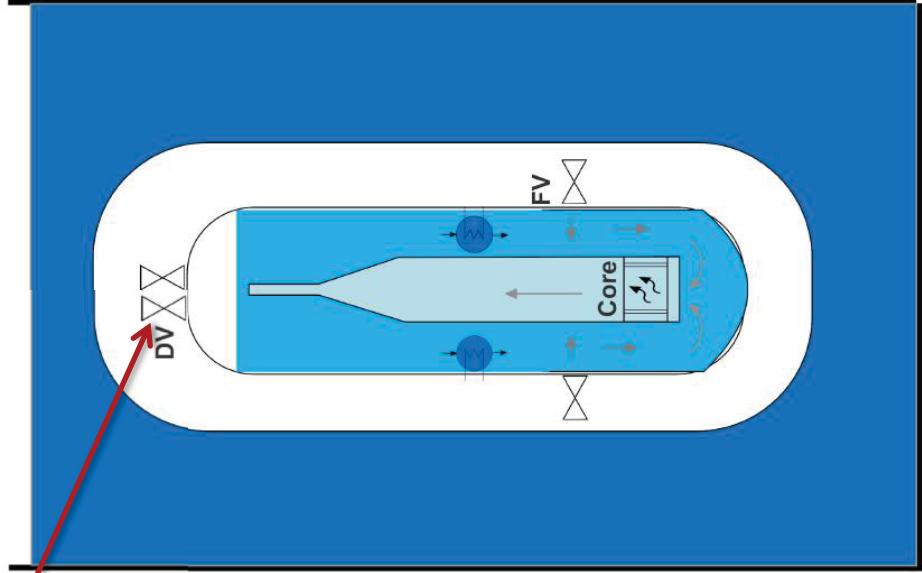


How to evaluate staffing requirements?

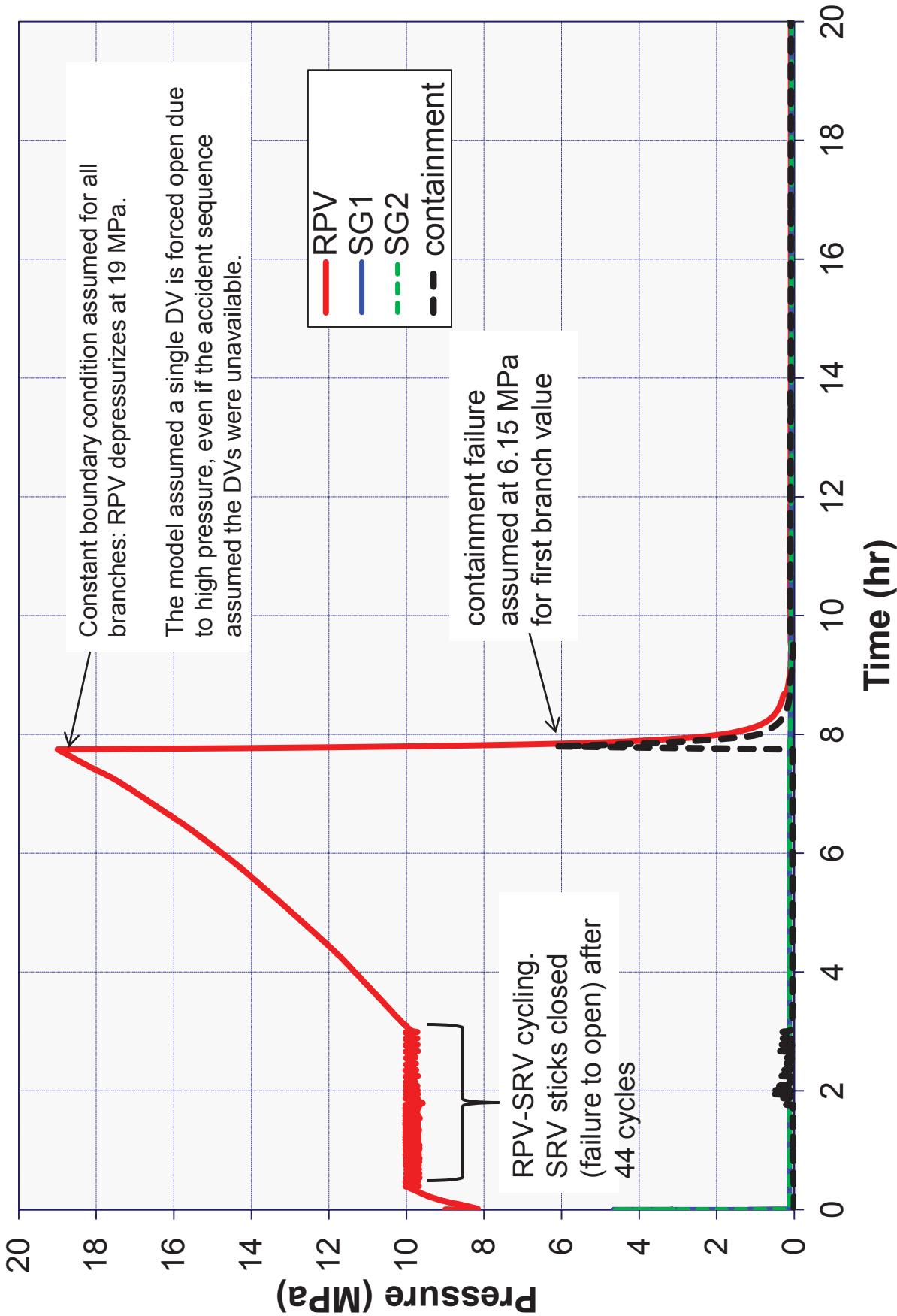


Are new Risk-Metrics Needed? DV failure example

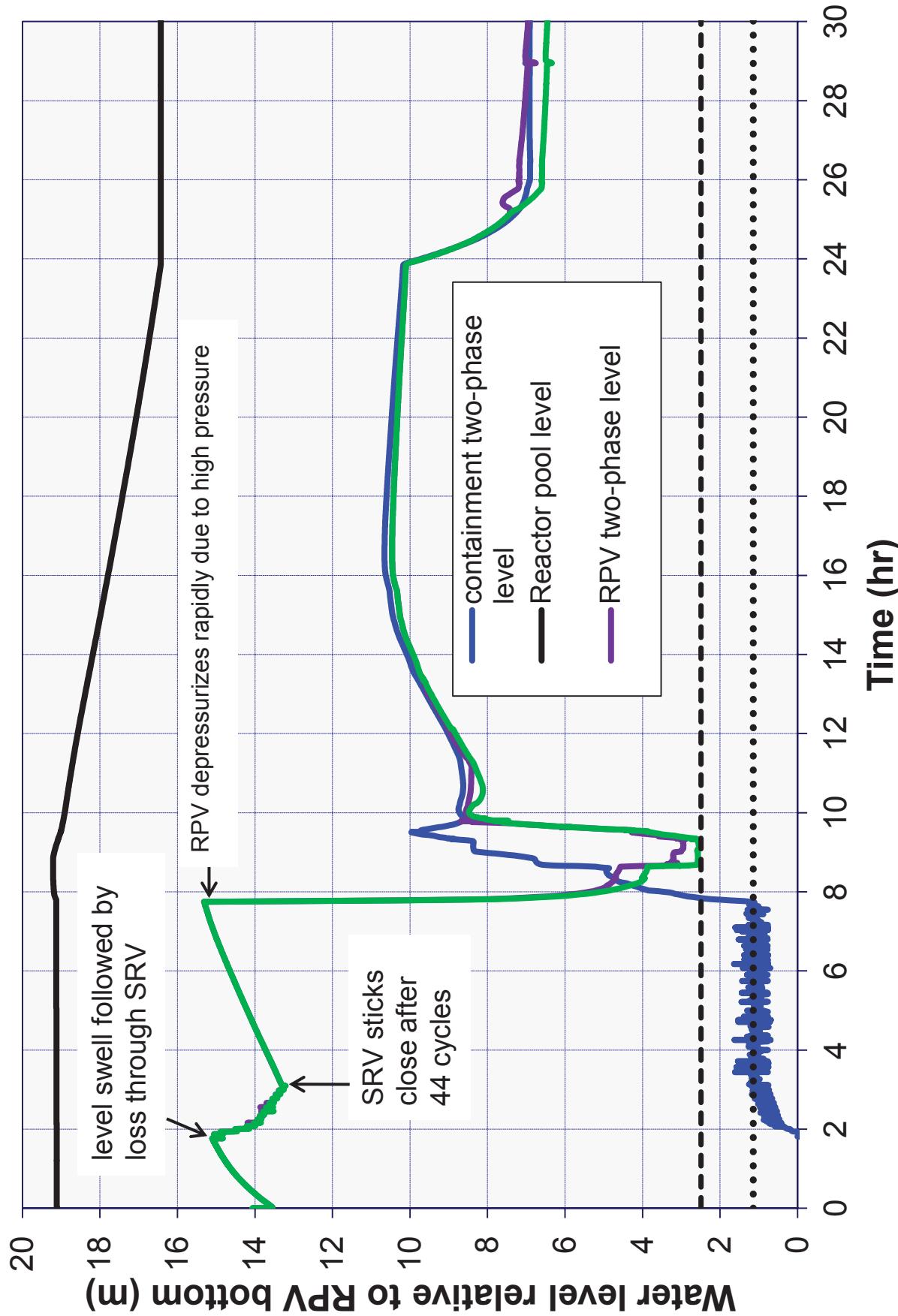
- A CVCS letdown can either be:
 - intentional to avoid containment overfilling (success branch) or
 - Unintentional Loss Of Coolant Accident (LOCA) to the reactor building (fail branch)



Primary, secondary, and containment pressures



Water levels in RPV, containment, and Rx pool



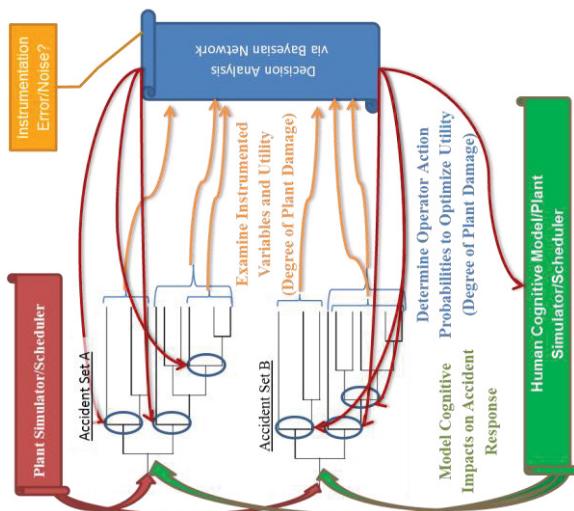
In the previous example:

- Two layers of Defense in Depth was lost:
 - Containment
 - Primary Pressure Boundary
- BUT:
 - No fuel rod failure was predicted by MELCOR
- Is this truly an OK end state? Would a regulator be satisfied?

Conclusions

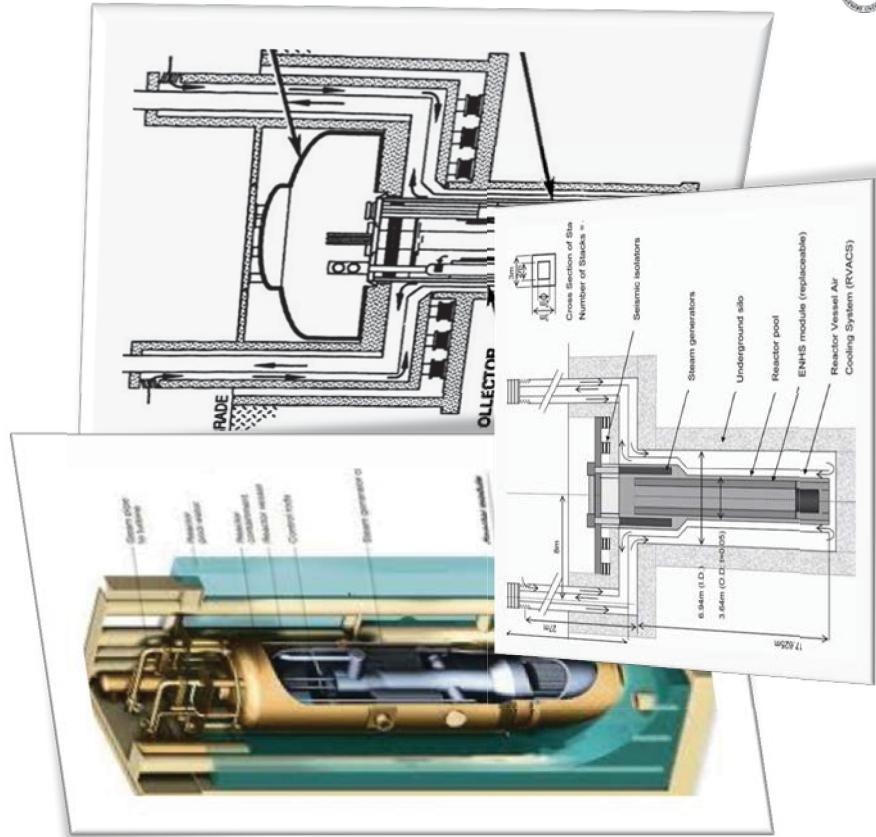
- SMRs provide many safety advantages over traditional LWRs, but justifying regulatory changes will be difficult
- The fundamental decision problems posed by SMR induced regulatory changes may not be answerable by traditional metrics such as

- Core Damage Frequency (CFD) and
- Large Early Release Frequency (LERF)
- New problems demand new analysis techniques integrating all of the following:
 - Safety Analysis
 - Cognitive Sociology
 - Decision Support



Review of Passive System Reliability Modeling Approaches for aSMRs

Dave Grabaskas (ANL)
Tanju Sofu (ANL)



Motivation and Scope

Open Issues

Methods Overview

Future Work

Motivation and Scope

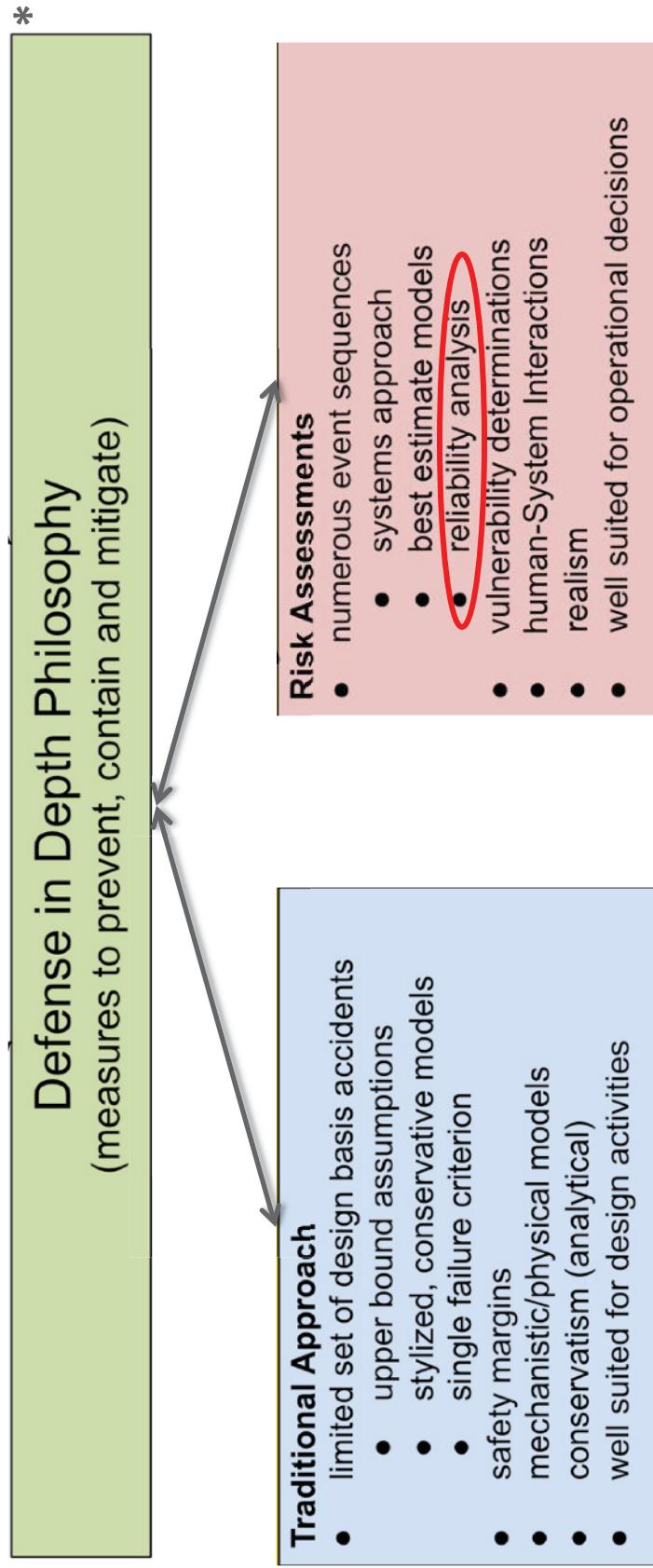
Open Issues

Methods Overview

Future Work



Motivation



Analysis of passive system reliability can be more complex than active components because of the difference in failure mechanisms

* Figure from NUREG-2150 – A Proposed Risk Management Framework

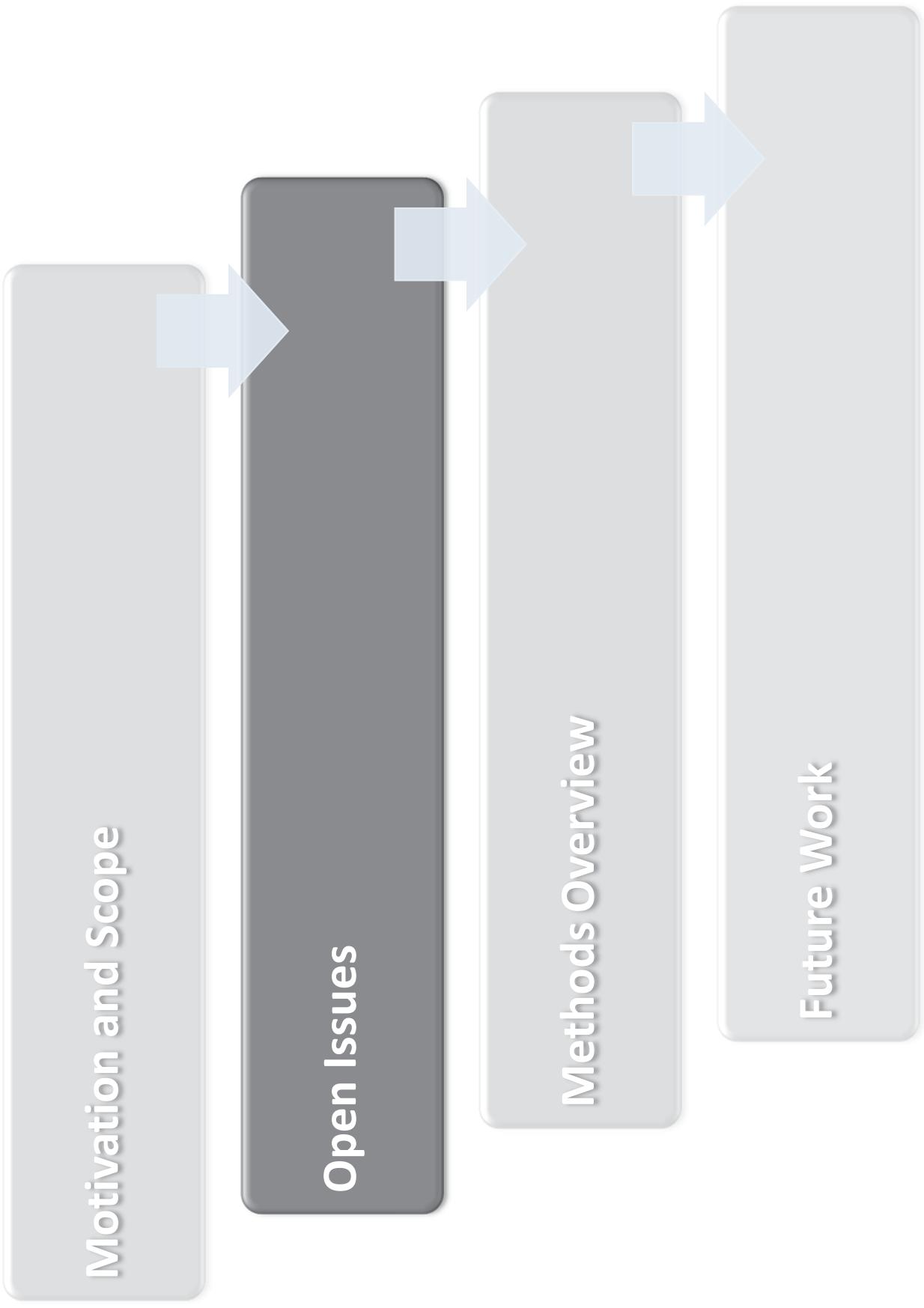


Motivation

Risk-informed regulation presents both challenges and opportunities for aSMRs that depend heavily on passive systems for safety functions

Scope

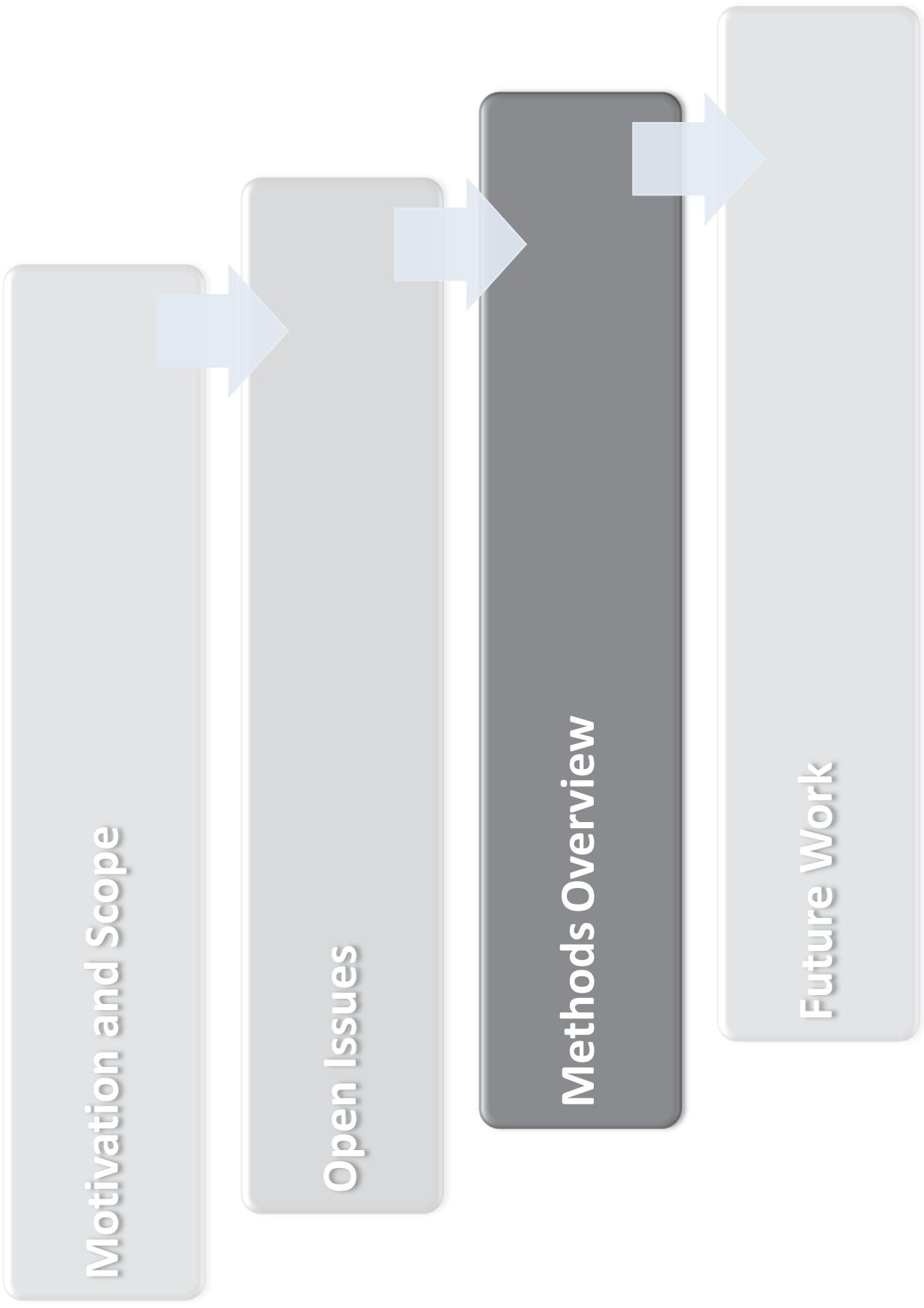
Review of existing approaches for modeling
reliability of passive safety systems, specifically
those which use natural circulation



Open Issues

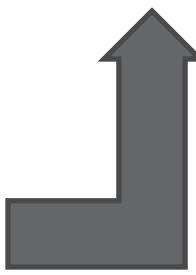
- **Functional Failure**
 - A system failure with no physical component failure
 - Difficult to model with classical event trees
- **Large Uncertainties**
 - New uncertainties due to possibility of functional failures
- **Dependency**
 - Large dependency on initial and boundary conditions (including other systems)
- **Dynamic Aspects**
 - Performance related to time-dependent conditions
- **Testing and Maintenance**
 - Unlike most active systems, online testing not possible





Methods - Margins Approach



- “Risk-based margins approach”
 - Used for AP600/AP1000/ESBWR
 - **Methodology**
 - 1) Conduct overall plant PRA
 - 2) Select “bounding” scenarios
 - 3) Identify high-impact variables
 - 4) Reanalyze scenarios using conservative assumptions
 - 5) Check margin
 - 6) Determine effect on overall risk
- 

Effect of passive reliability on overall risk is negligible

Methods - Margins Approach

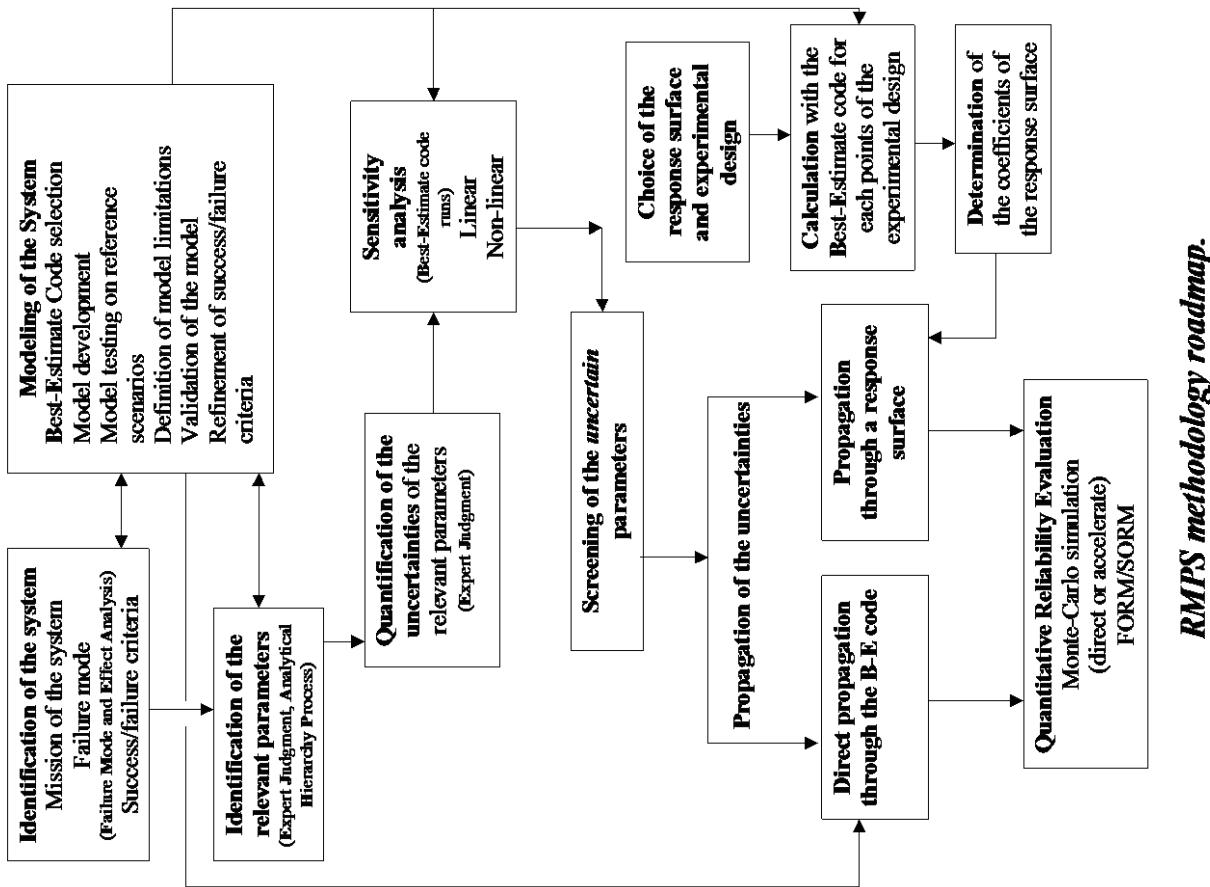
- **Pros**
 - Regulatory experience
 - Straightforward application
 - Uses current tools and codes

- **Cons**
 - Derivative of traditional, deterministic techniques
 - Use of conservative assumptions
 - Not a true reliability analysis

Methods - Mechanistic

- **Structured incorporation**
 - RMPS (Reliability Method for Passive Systems) – EU/CEA
 - APSRA (Assessment of Passive System ReliABILITY) – India





RMPs methodology roadmap.

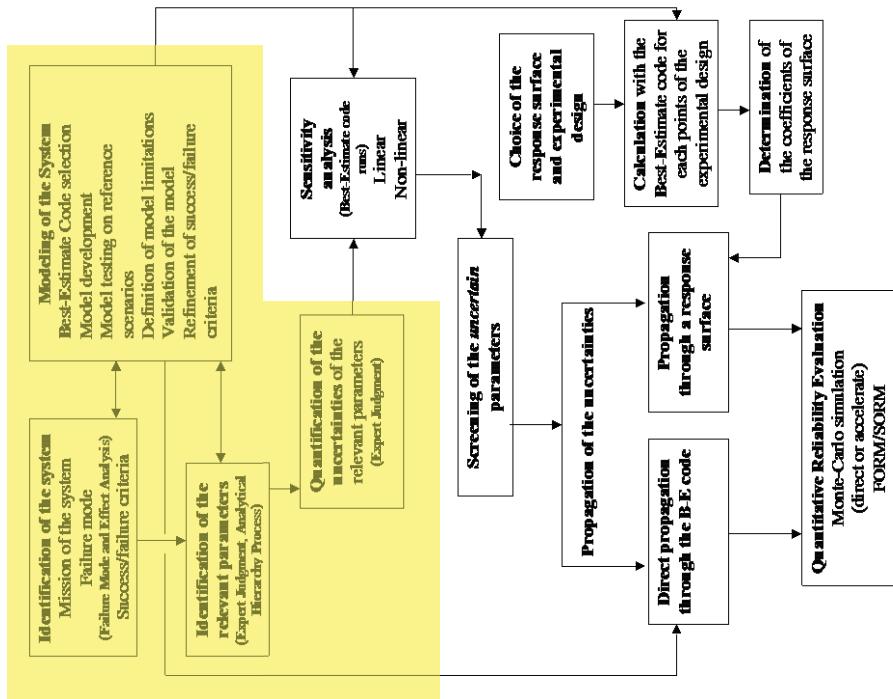


Methods - Mechanistic

1) Preprocessing/Model Development

- Identify system and mission
(such as PCT<2200 °F)
- Identify influential system parameters
- Create distributions for uncertainties

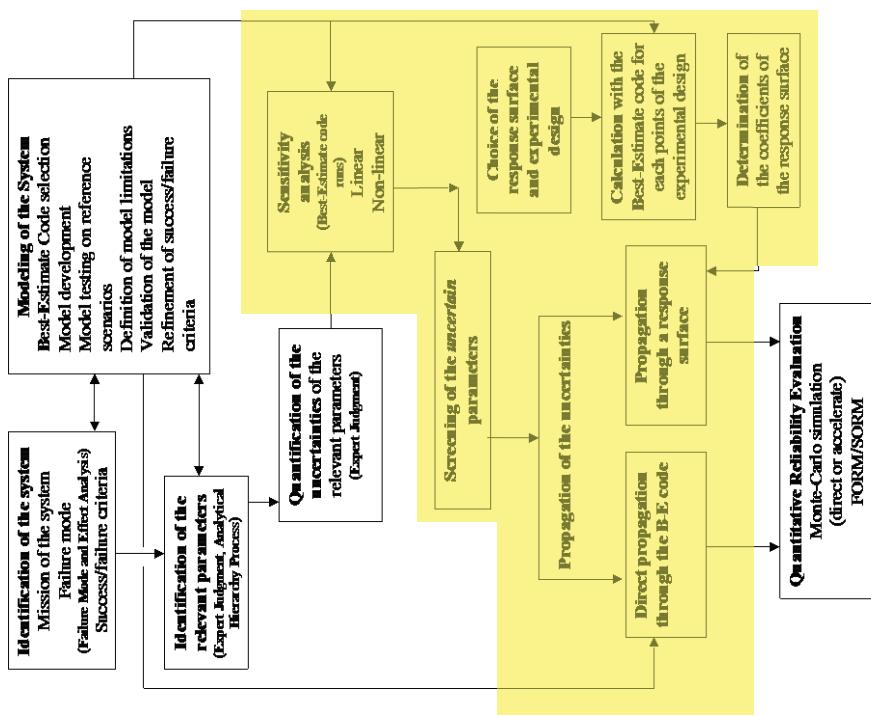
Structured expert elicitation
(FMEA, HAZOP, or AHP)



Methods - Mechanistic

2) Simulation and Uncertainty Propagation

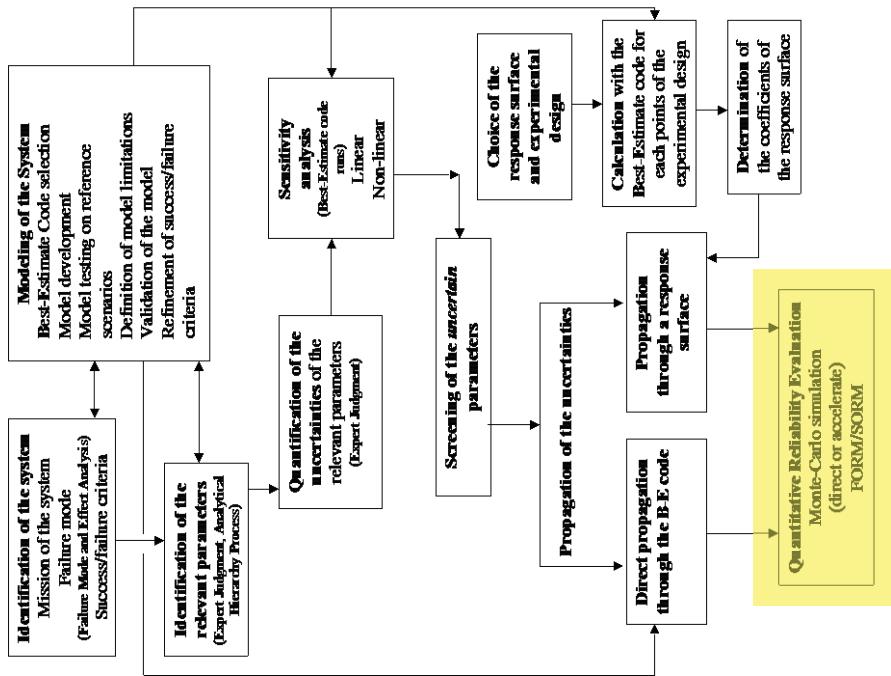
- Use system code or combination system/CFD code
- Propagate uncertainties using either Monte Carlo sampling or through creation of a response surface



Methods - Mechanistic

3) Analysis/Post-processing/Integration

- Conduct sensitivity analysis
- Incorporate results into PRA
- Create system failure event(s) on event trees



Methods - Mechanistic

- **Pros**
 - Structured approach to conducting true reliability analysis
 - Can be carried out using current tools
 - Fairly well-developed

- **Cons**
 - Still susceptible to many of the “open issues”
 - Trouble handling time/dependencies
 - Integration into PRA not straightforward (how to add degraded?)



Methods - Mechanistic

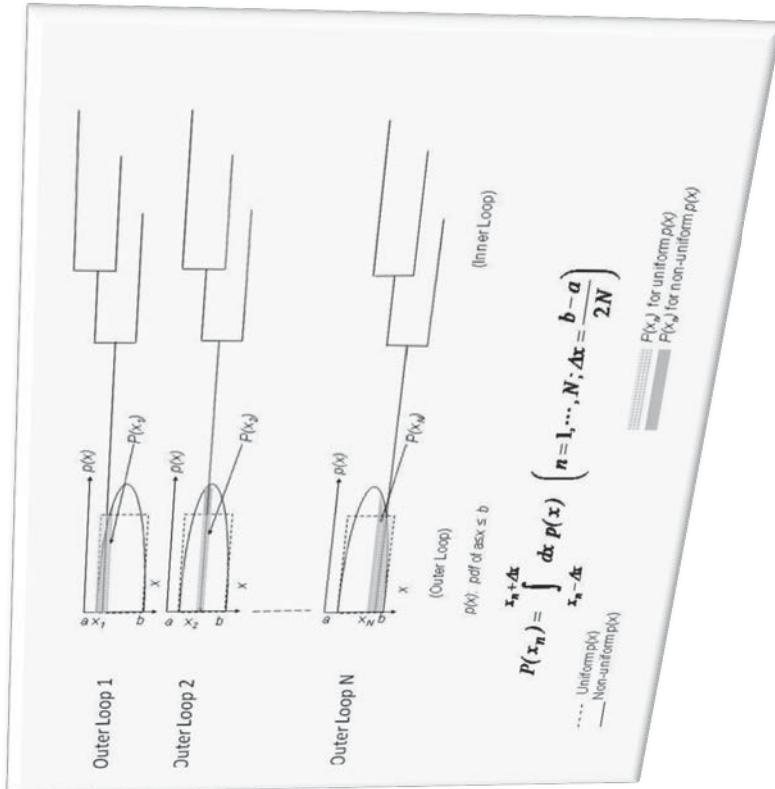
These guidelines highlighted the need for the development of dynamic event trees, as compared to conventional PSAs which do not systematically model the dynamic aspects of accident progression, including dynamic system interactions and dependencies and thermal hydraulic phenomena induced failures. This requirement emerges from the consideration that thermal hydraulic natural circulation passive system operation is strongly dependent, more than other safety systems, on the state/parameter evolution of the system during the accident progression.

- RMPS Project: Final Report



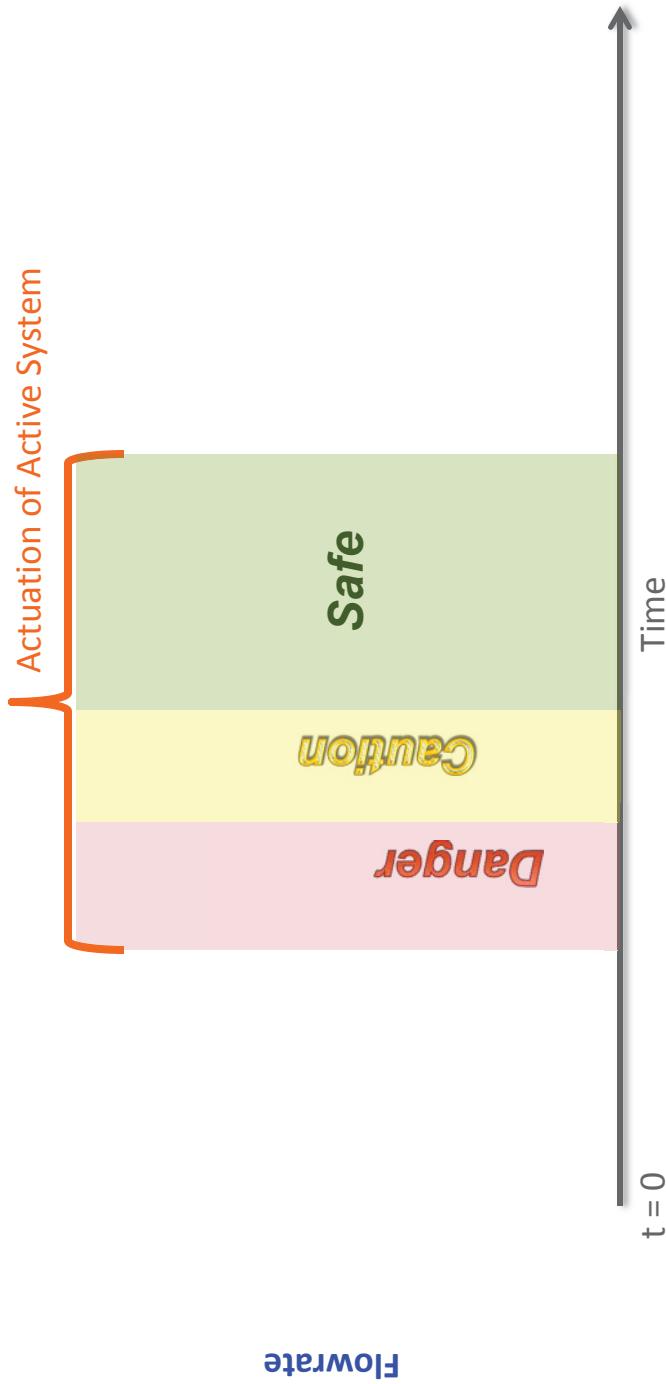
Methods - Dynamic

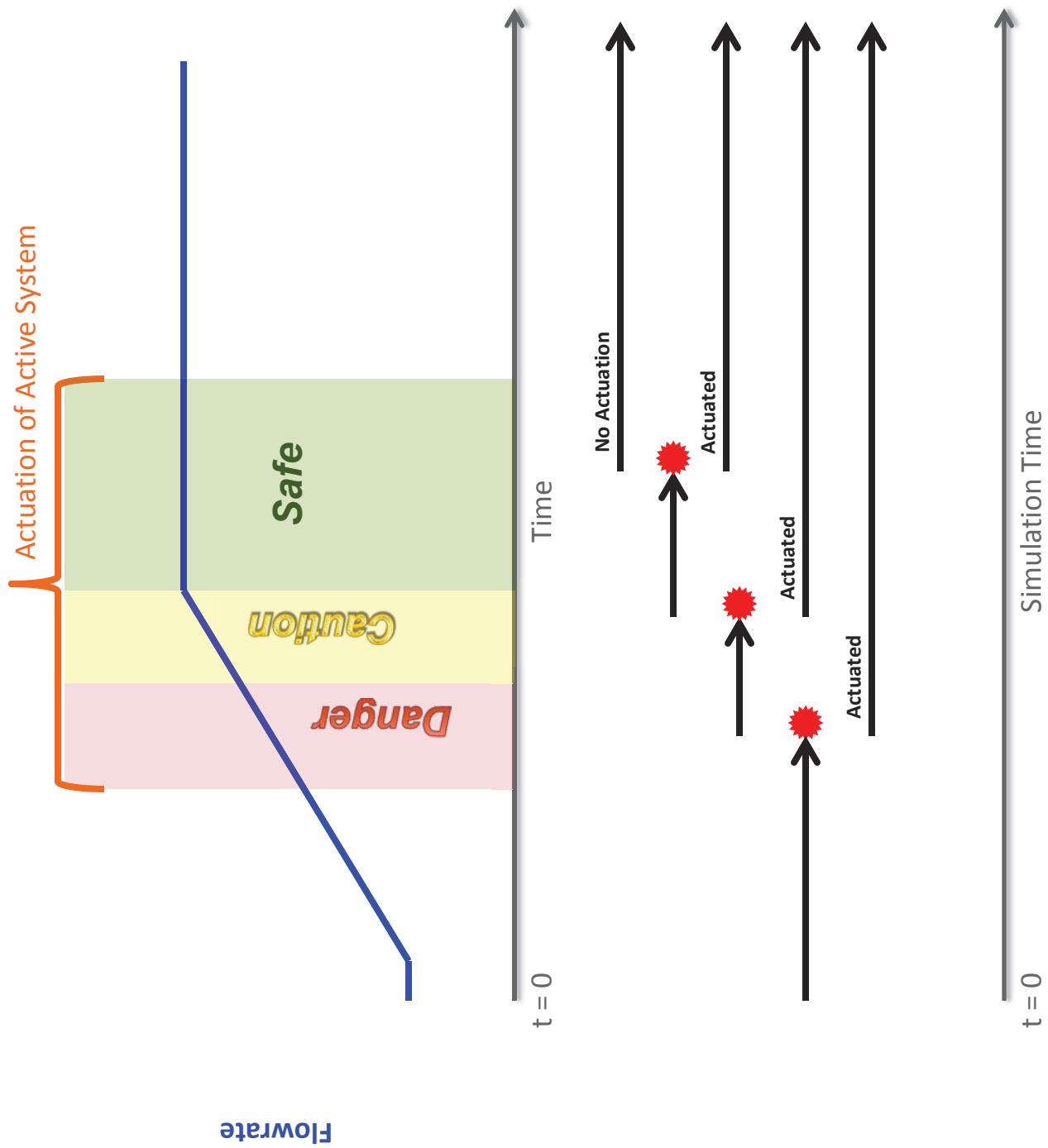
- Such as dynamic event trees
 - Use same expert elicitation to develop uncertainties
 - Allow dynamic analysis to propagate uncertainties and create branching trees



Methods - Dynamic

- Example
 - SFR post loss of flow accident
 - Natural circulation in the vessel keeps core cool
 - Circulation takes some amount of time to develop





Methods - Dynamic

- **Pros**
 - Phenomenologically consistent treatment of time
 - Resolves dynamic and dependency aspects
 - Integration into PRA

- **Cons**
 - Development and regulatory approval
 - Data management and interpretation

Motivation and Scope

Open Issues

Methods Overview

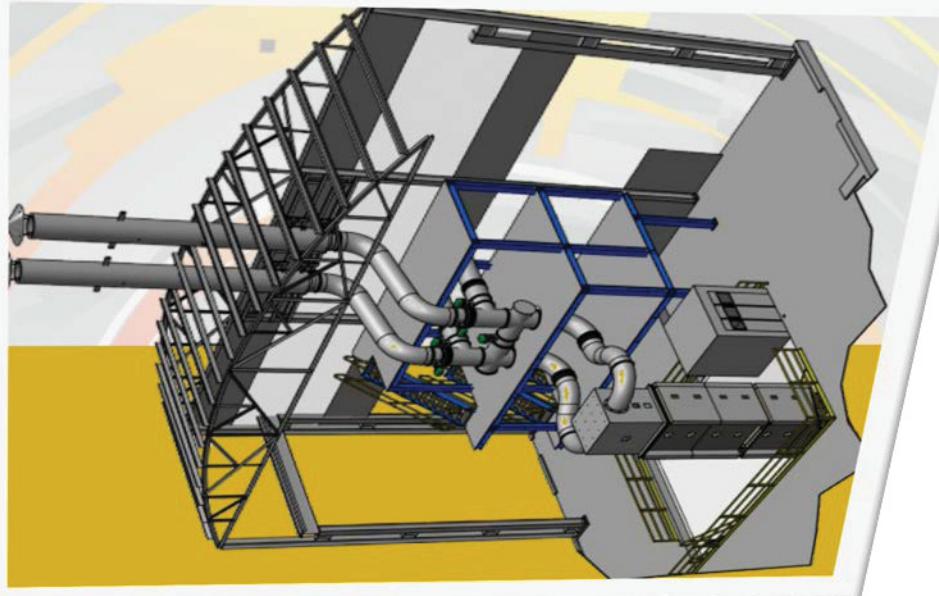
Future Work



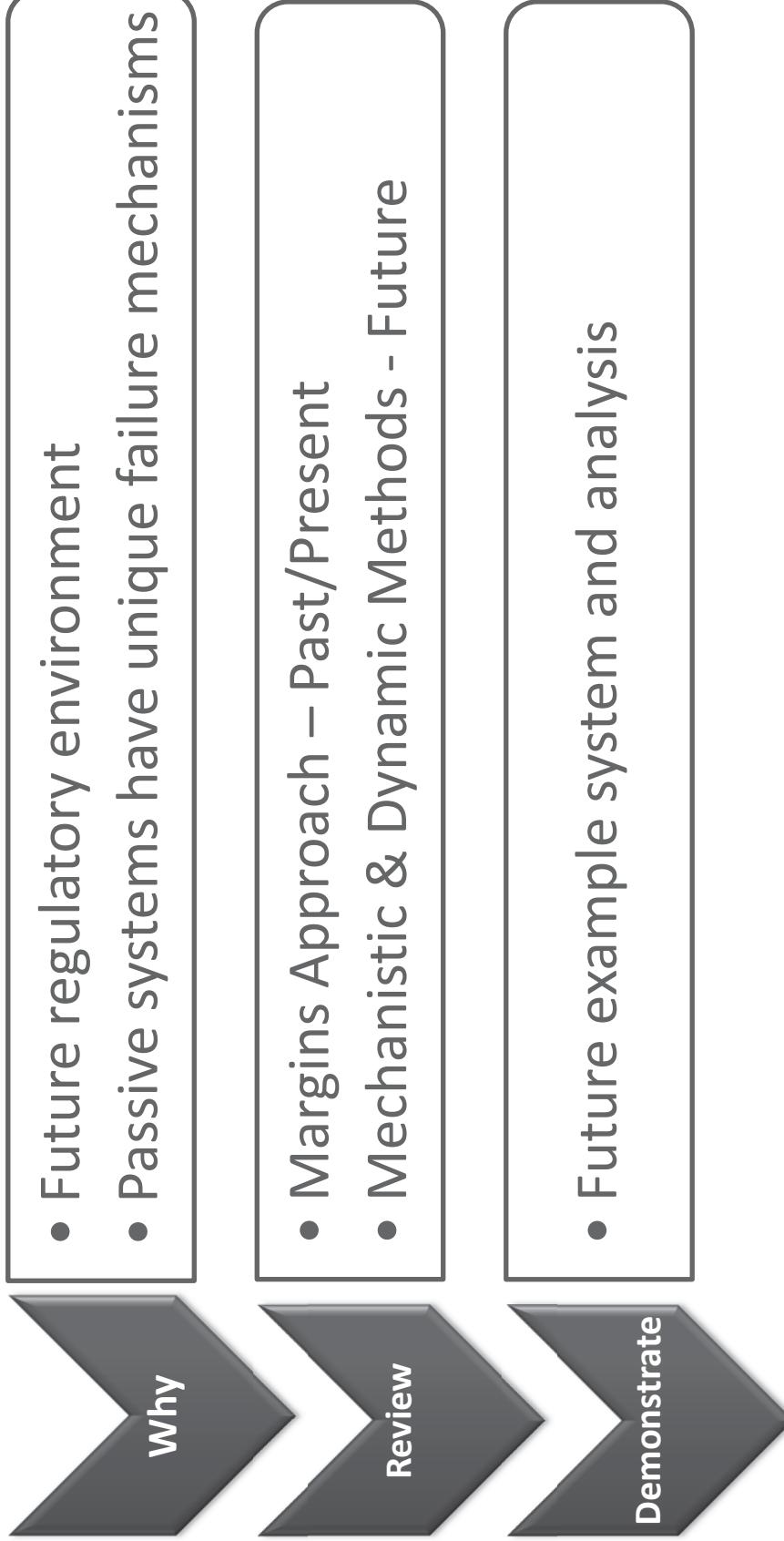
Methodology Demonstration

■ Next steps

- Create example system
 - Use NSTF at Argonne
- Carry out example analysis
 - Using mechanistic and dynamic methods
- Compare to regulatory goal
 - Risk-informed safety margin characterization

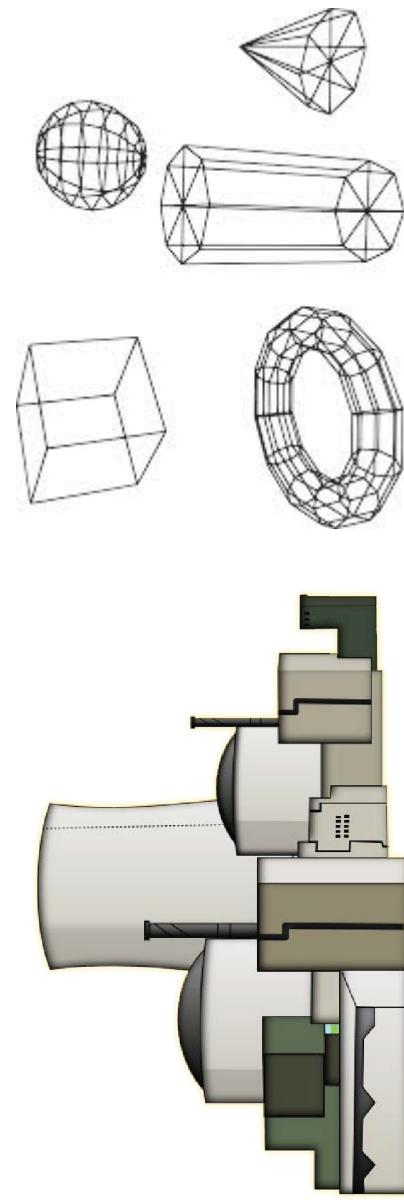


Summary



3D Simulation with PRA *(Probabilistic Risk Analysis)*

Aug 2013





Idaho National Laboratory

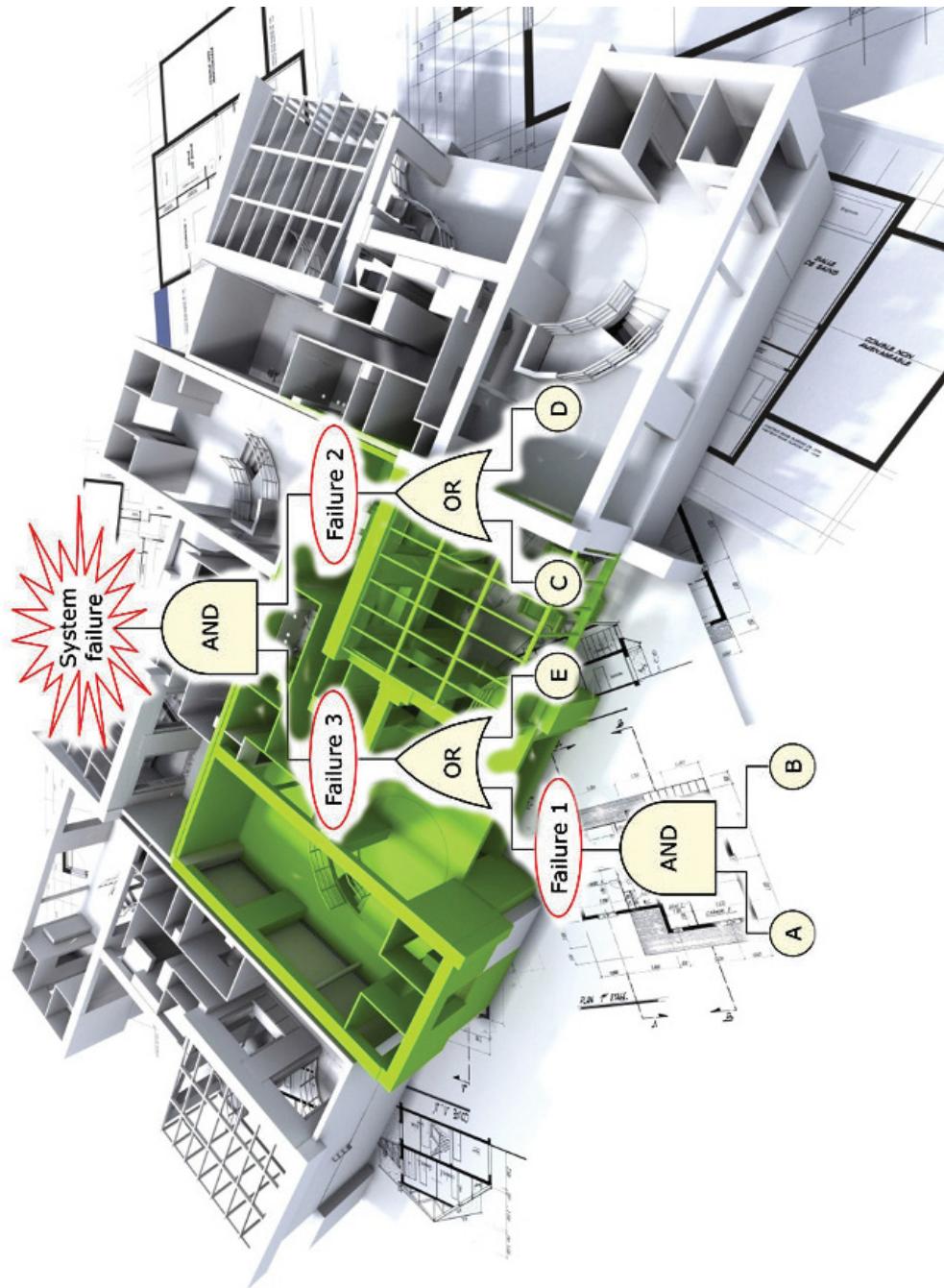




Idaho National Laboratory

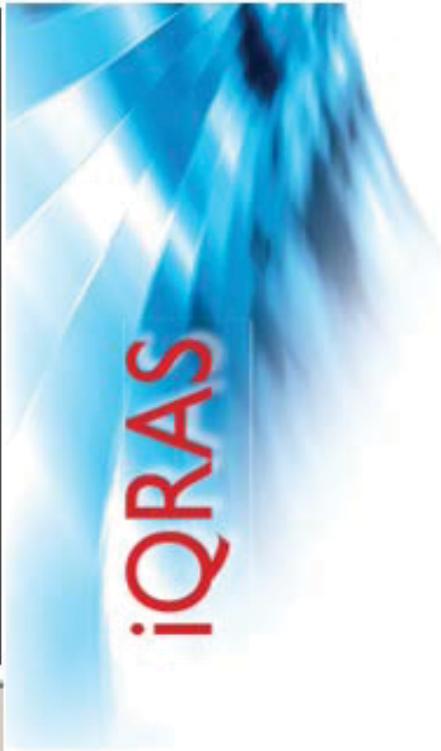
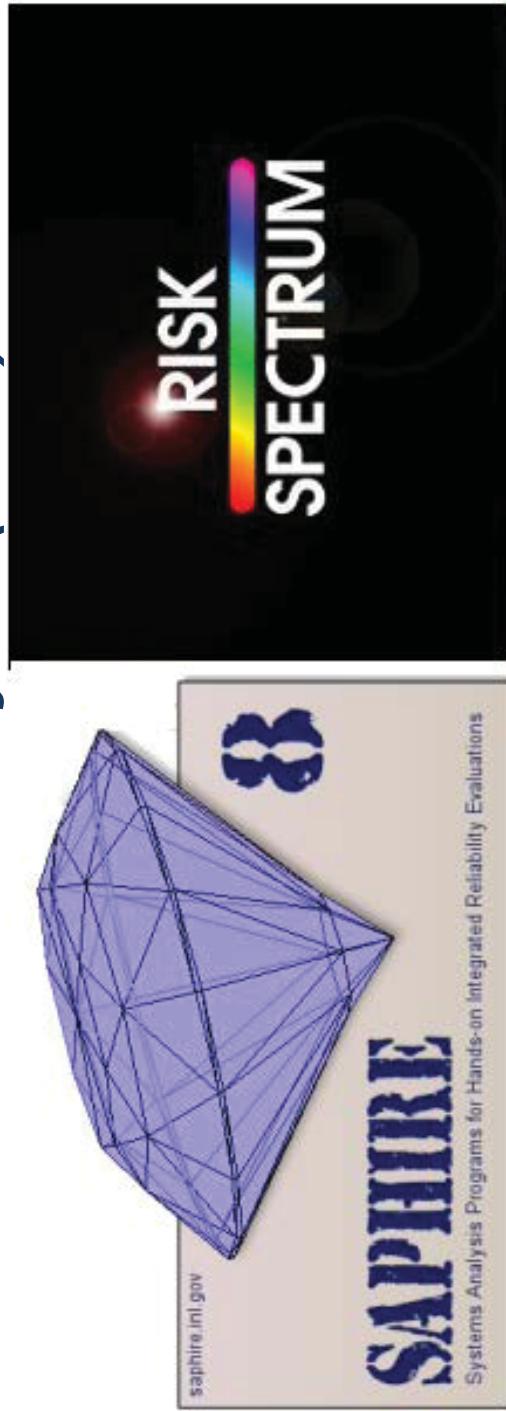
$$\Delta \mathbf{X} = \mathbf{X}_f - \mathbf{X}_i \quad \Delta \mathbf{v} = \mathbf{v}_f - \mathbf{v}_i \quad \omega = \frac{\Delta \theta}{\Delta t} \quad \sigma = \frac{\Delta \omega}{\Delta t}$$
$$\bar{\vec{v}} = \frac{\Delta \vec{r}}{\Delta t} \quad \bar{\vec{a}} = \frac{\Delta \vec{v}}{\Delta t}$$
$$\mathbf{V} = \mathbf{V}_0 + \vec{at} \quad \mathbf{x} = \mathbf{x}_0 + \mathbf{v}_0 t + \mathbf{a} t^2 / 2$$
$$\mathbf{v}^2 - \mathbf{v}_0^2 = 2 \mathbf{a} (\mathbf{x} - \mathbf{x}_0)$$
$$\bar{v} = \frac{\mathbf{v}_f + \mathbf{v}_i}{2} \quad \Delta \mathbf{x} = \bar{v} \Delta t$$
$$\mathbf{F}_{\text{tot}} = m \mathbf{a}$$
$$E = K + U$$
$$W = F d_{\parallel} = F_i d$$
$$W_{\text{tot}} = \Delta(\text{KE})$$
$$\Delta U = -W_f$$
$$\frac{1}{2} k x^2 \quad \omega = \sqrt{\frac{k}{m}}$$
$$\mathbf{p} = m \mathbf{v}$$
$$\vec{P}_{\text{tot}} = \vec{P}_{\text{final}}$$
$$\left(\sum_j \mathbf{m}_j \hat{v}_j \right)_{\text{tot}} = \left(\sum_j \mathbf{m}_j \hat{v}_j \right)_{\text{final}}$$
$$\mathbf{v} = |\mathbf{v}| \hat{v} \quad v = \sqrt{v_x^2 + v_y^2}$$
$$\mathbf{v} = v \sin(\theta) \hat{i} + v \cos(\theta) \hat{j}$$
$$\mathbf{v} \rightarrow \mathbf{x}, \mathbf{y} \quad \mathbf{x}_0 \rightarrow \mathbf{x}_0, \mathbf{y}_0$$
$$\mathbf{v} \rightarrow \mathbf{v}_x, \mathbf{v}_y \quad \mathbf{v}_0 \rightarrow \mathbf{v}_{0x}, \mathbf{v}_{0y}$$
$$\mathbf{a} \rightarrow \mathbf{a}_x, \mathbf{a}_y$$
$$\mathbf{v} = \lambda f$$
$$a = \frac{v}{R}$$
$$x = A \cos(\omega t) \quad v = A \sin(\omega t)$$
$$y = A \sin(\omega t) \quad v = A \cos(\omega t)$$
$$\theta = \tan^{-1} \left(\frac{v_y}{v_x} \right)$$
$$\theta = \cos^{-1} \left(\frac{v_x}{v} \right)$$
$$\theta = \sin^{-1} \left(\frac{v_y}{v} \right)$$
$$\theta = \pi - \theta$$
$$v = \omega r$$
$$a = \alpha r$$
$$I = \sum_i m_i r_i^2 \quad \theta = \theta_0 + \omega_0 t + \frac{1}{2} a t^2$$
$$\omega^2 - \omega_0^2 = 2 \alpha (\theta - \theta_0)$$
$$L = \pi p = m v r_{\perp} \quad \tau = r_{\perp} F = r_{\perp} \alpha$$
$$L = H \alpha \quad \tau = \frac{\Delta L}{\Delta t} \quad \tau = I \alpha$$
$$\sum_i \bar{F}_i = 0 \quad \sum_i \bar{\tau}_i = 0$$
$$\Delta Q = (\text{quant.}) C_{\text{cool}} \Delta T \quad \Delta S \geq 0$$
$$\Delta Q_{\text{in}} = \Delta W_{\text{by}} + \Delta E$$
$$C_p = C_v + R$$
$$\frac{RT}{2} \mid \text{deg freedom}$$
$$x = A \cos(\omega t) \quad v = A \sin(\omega t)$$
$$y = A \sin(\omega t) \quad v = A \cos(\omega t)$$
$$a = -A \omega^2 \cos(\omega t) \quad \dot{a} = A \omega^2 \sin(\omega t)$$
$$\frac{GM}{r^2} = g R_e \quad \frac{GMm}{r^2}$$
$$M_e = 5.97(10)^{24} \text{ kg} \quad R_e$$
$$R_e = 6.37(10)^6 \text{ m} \quad -\frac{GMm}{r}$$
$$G = 6.67 (10)^{-11} \text{ N m}^2/\text{kg}^2$$
$$B = \rho_{\text{eq}} V_{\text{disk}} g$$
$$A_1 v_1 = A_2 v_2$$
$$P + \frac{1}{2} \rho v^2 = \text{const}$$

Combining Both Worlds



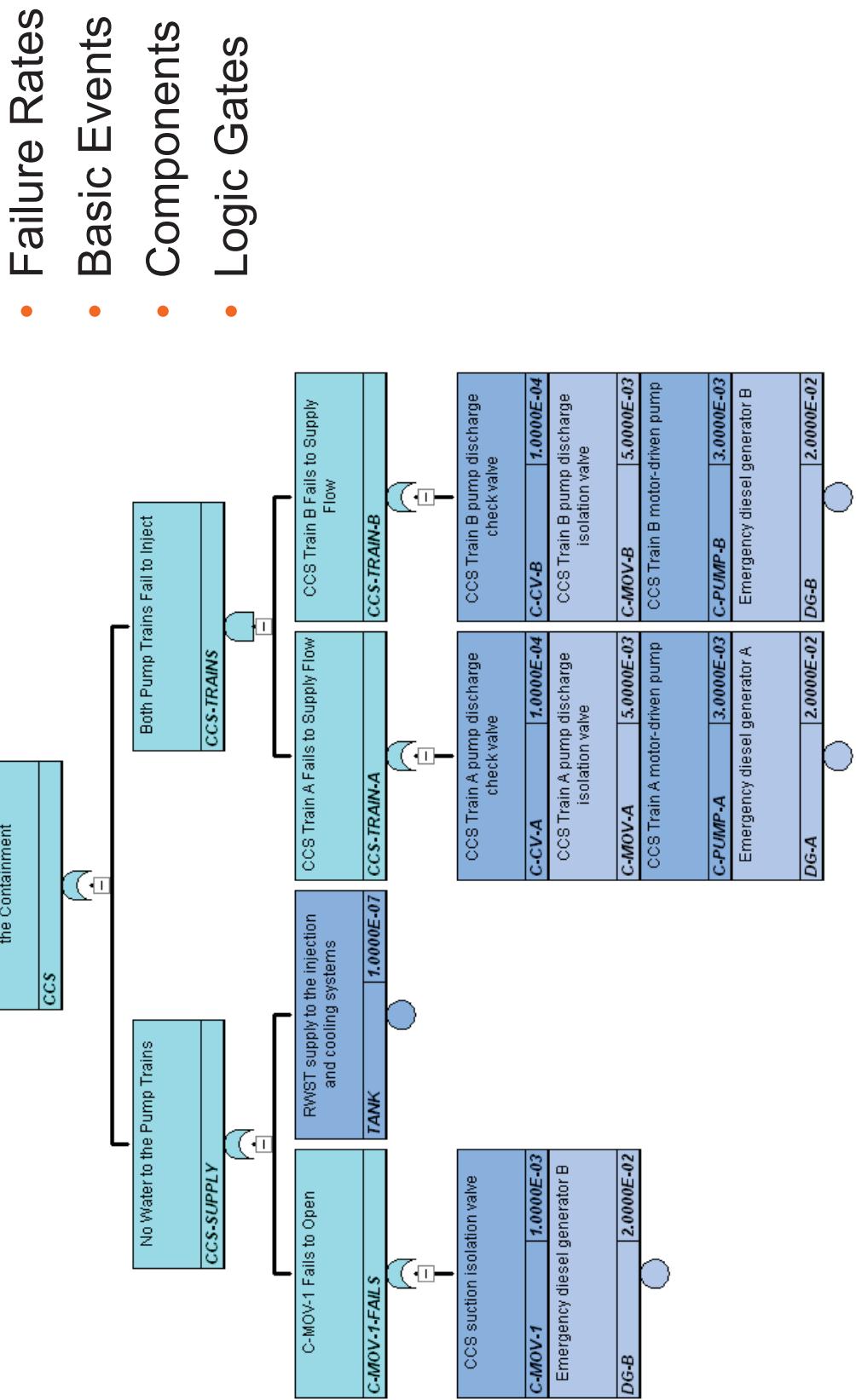


Probabilistic Risk Analysis (PRA)



CAFTA
Fault Tree Analysis System

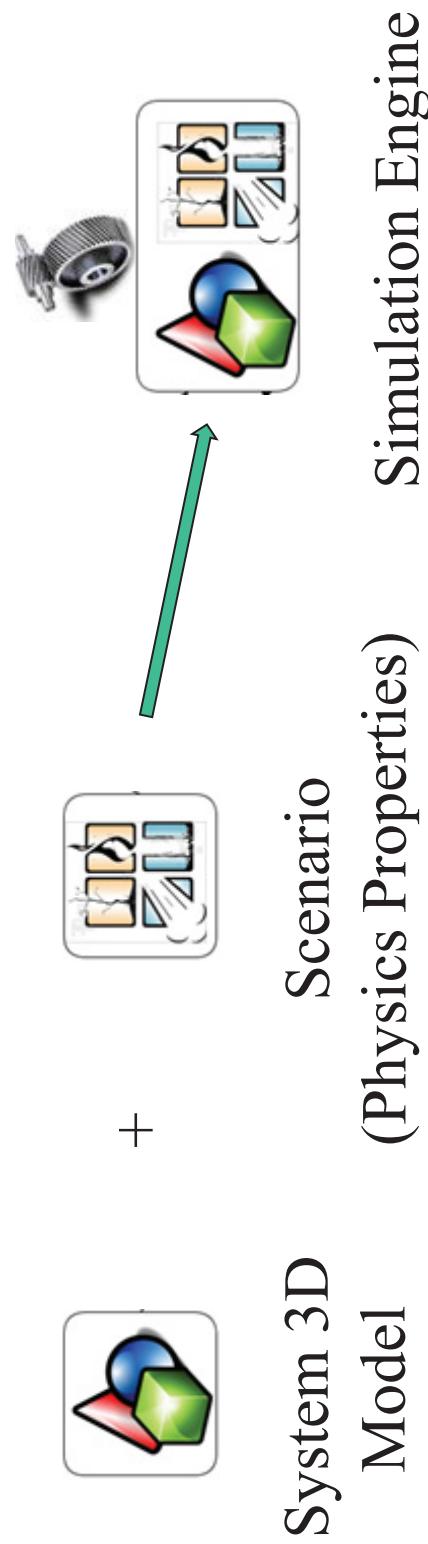
Fault Tree Analysis



Limitations

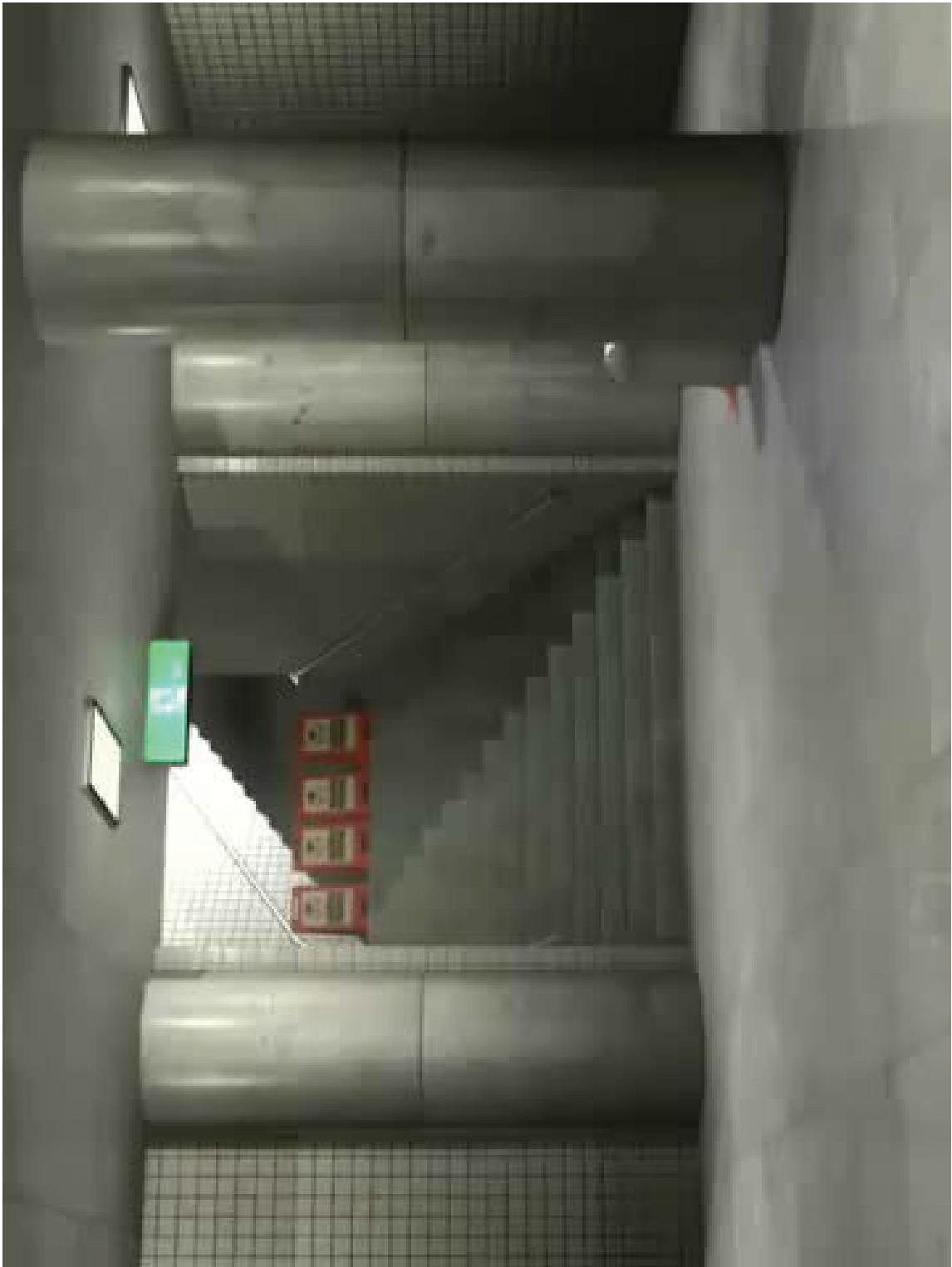
- You can only model understood or foreseen issues in a system.
- Difficulty in determining some Common-Cause or Common-Mode failures
- Location issues of components hard to model
- Environmental effects nearly impossible to accurately capture

3D Physics Simulation



Possibilities ?

Water





Wave

"R&D" 2012-2013



Wind





Idaho National Laboratory

Breaking / Destruction



Fire ?

- Currently only Visual
- Development being done on fire spread/consuming
- Set property of model items to determine combustion attributes

3D Simulation Packages and Environments

- Unreal
- Maya
- 3D Studio Max
- Houdini
- Real Flow
- Blender

Each has advantages and disadvantages.

3D Simulation Limitations

- Years of experience to become proficient
- 3D modelers lack knowledge of important components
- Hard to link new events/impacts to component failures
- Not probabilistic in nature, either occurs or does not
- Long simulation times

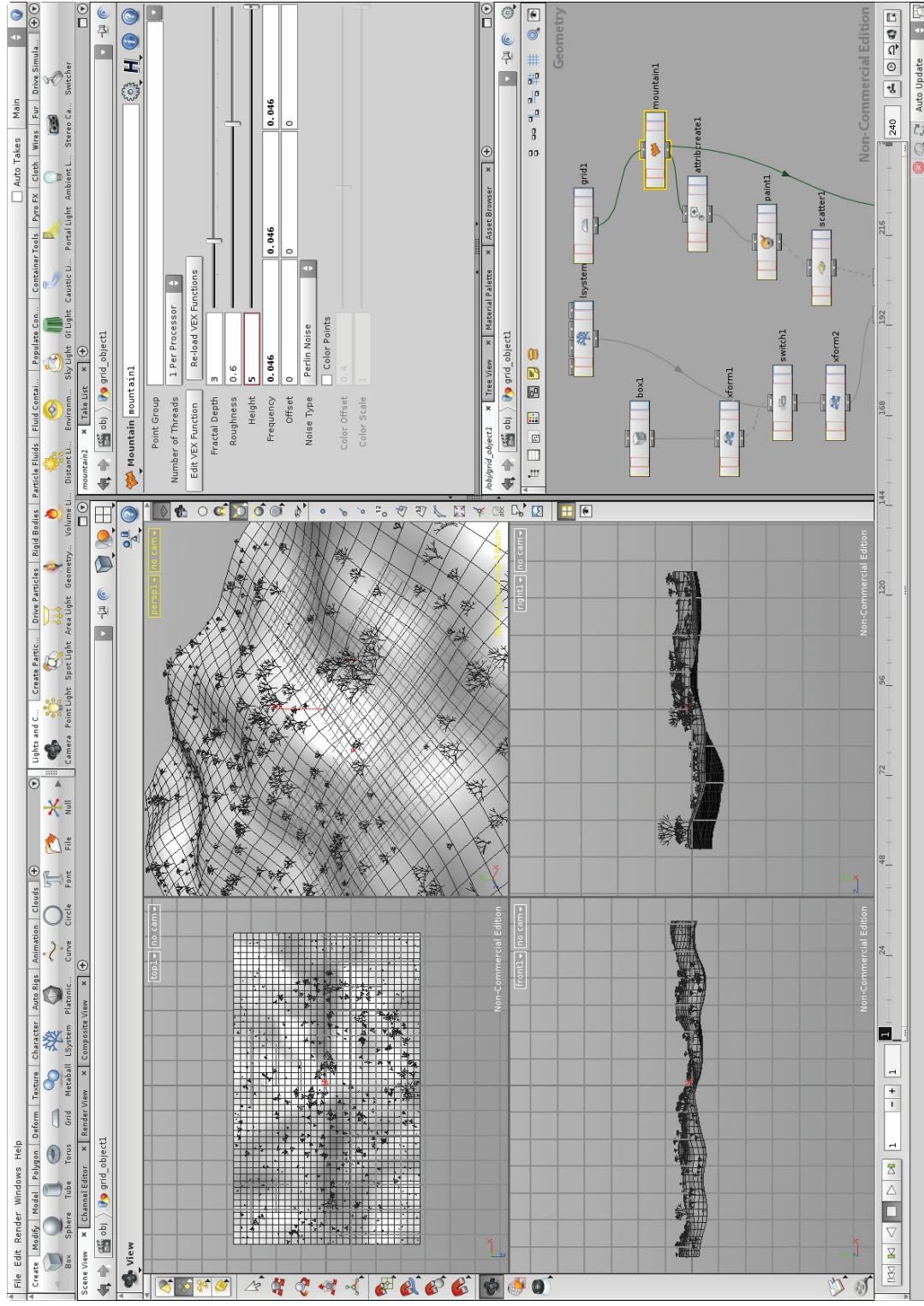
Use the Strengths of both sides

- Traditional PRA
 - Modeling event and component interactions in the system
 - Probability of component failures in a given state
 - Split simulation based on key failure points
- 3D Physics Simulation
 - Physics based common cause component failures
 - Unforeseen location based failures or protections
 - Structure design effects
 - More accurate timeline for component failures

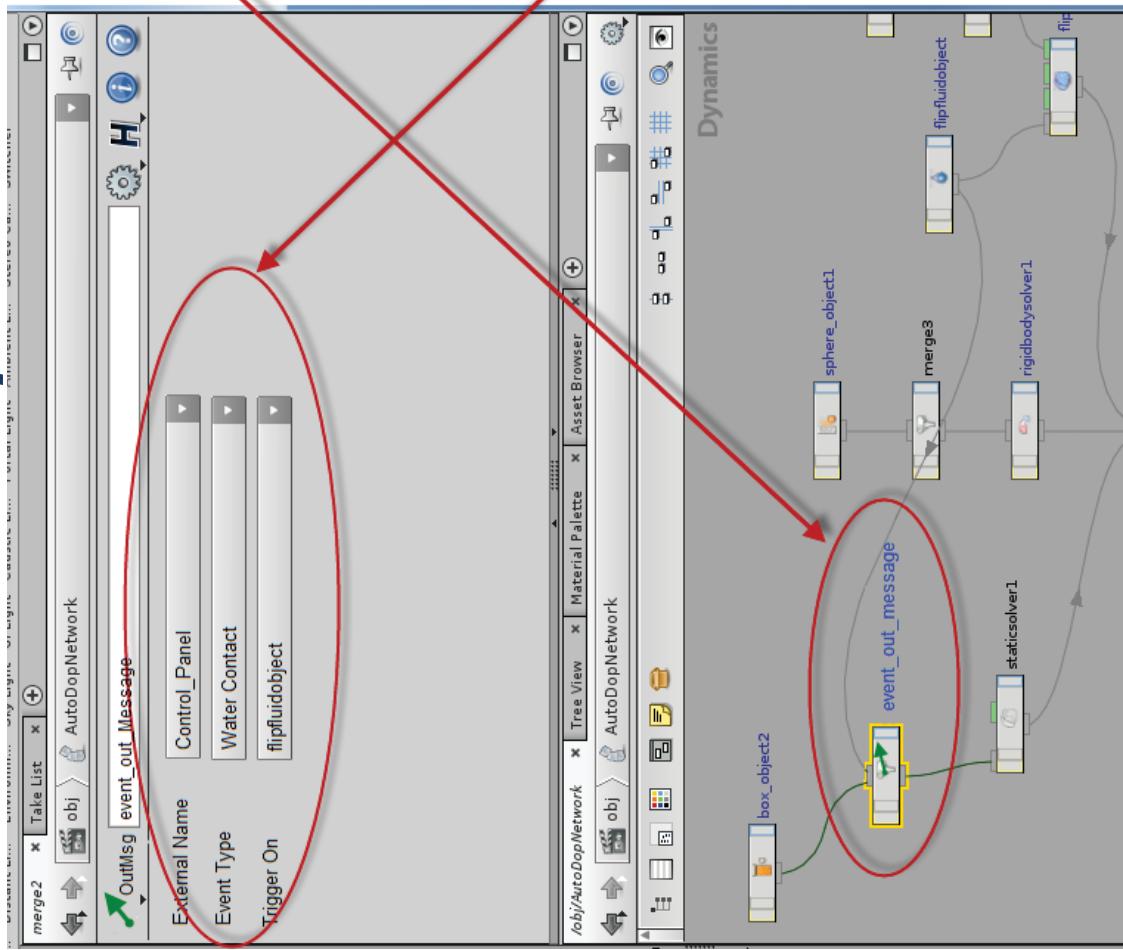
Houdini by Side Effects

- Highly versatile
- Good simulation engine
- Can handle complex modeling
- External communication capabilities
- Vast array of Physics capabilities
- Simple Operators to manipulate objects (can be Custom made)

Interface



Customizable Operators



Custom Operator for
sending out a message
on an event trigger

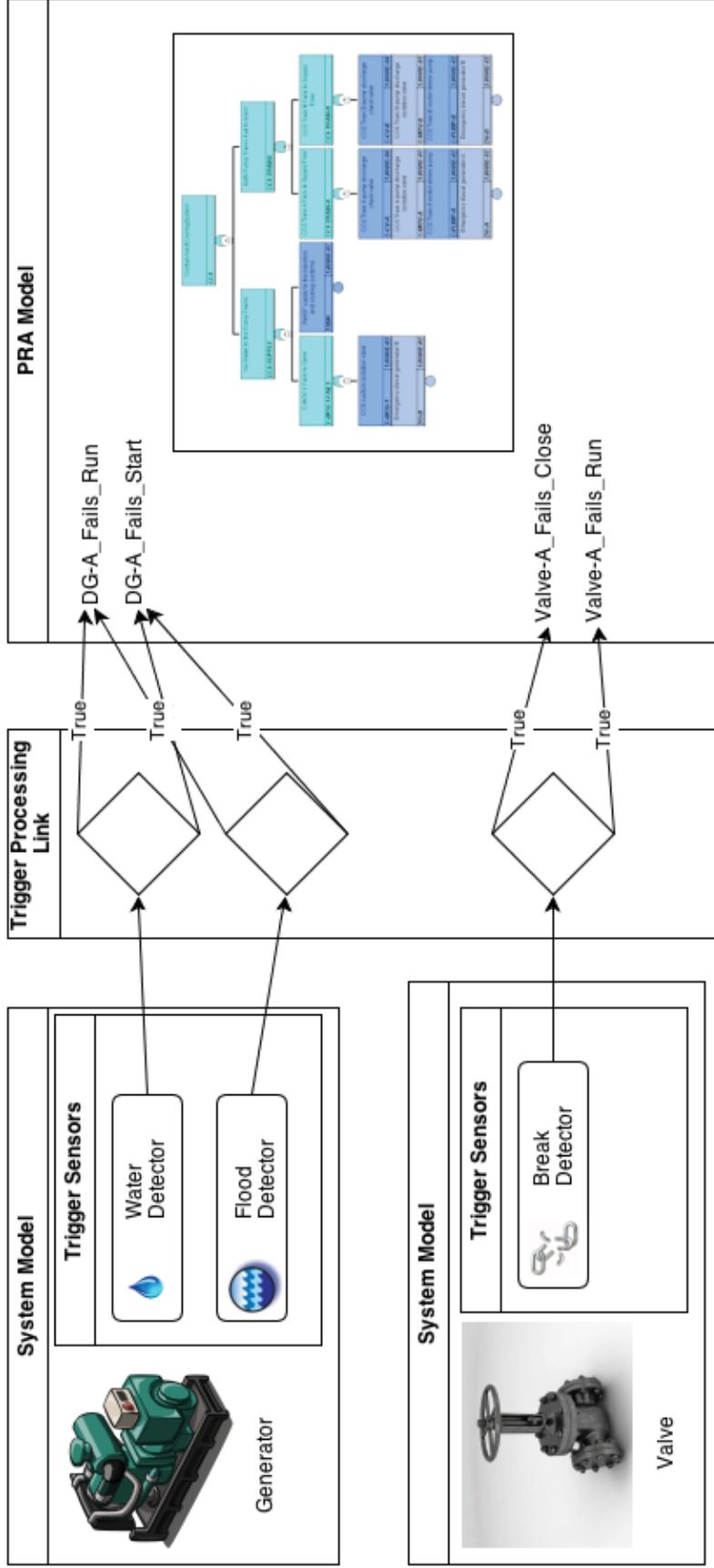
Operator properties

External Communication
done with Python code
and Sockets



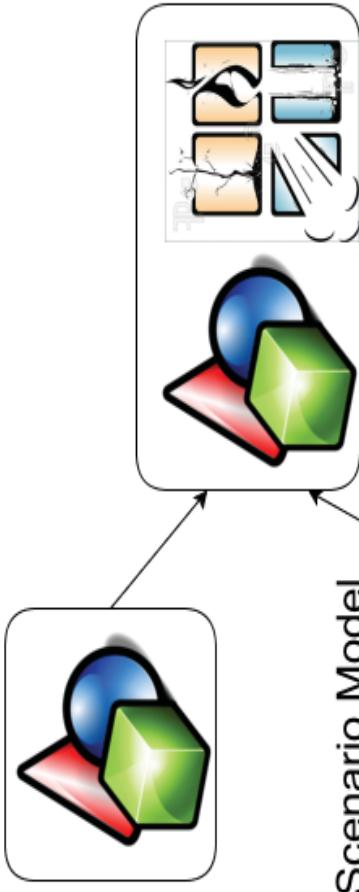
Idaho National Laboratory

Establishing Communication

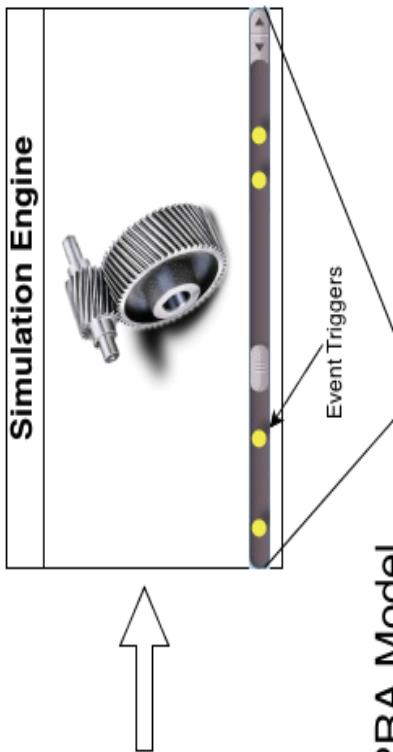
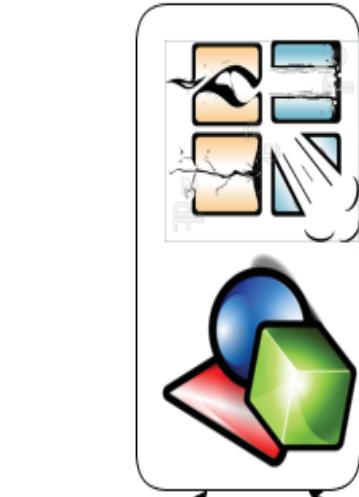


Linking Traditional PRA with 3D Simulations

System Model



Scenario Model



Goals

- Determine unforeseen possible design issues
- Provide a means of testing mitigation options
 - Test natural disaster scenarios

Obstacles

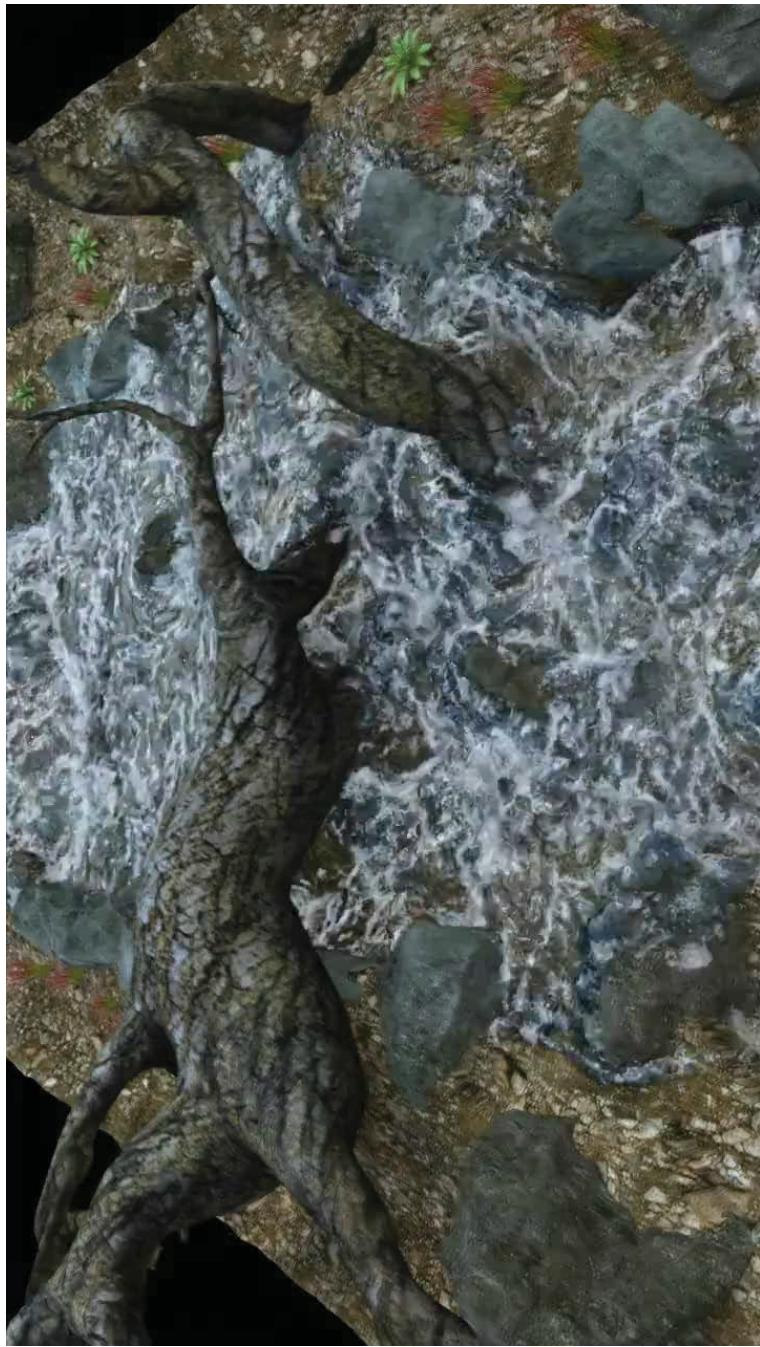
- 3D modelers need design plans for modeling
- Modifications by modelers need to me made for each scenario to be run.
- Simulation Time – simulations can take weeks to run on high performance multi processor machines. (Depending on complexity of the model and applied physics)
- Some simulation engines require them to be run on a single machine, distributed processing options reduces accuracy because of one step information lag from other calculations.

Traditional 3D steps

- Data Assembly (Preprocessing the model)
- Simulation (Physics and motion of 3d Objects)
- ~~Surfacing (Apply texture, lighting, effects)~~
- ~~Rendering (Create video or images)~~

Typical Simulation Times

- ~1 min per frame
 - Medium sized room with high detail
 - Dual processors (12 cores total) 48 GB ram



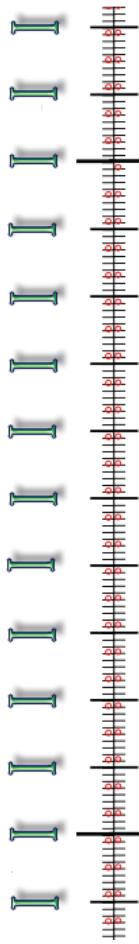
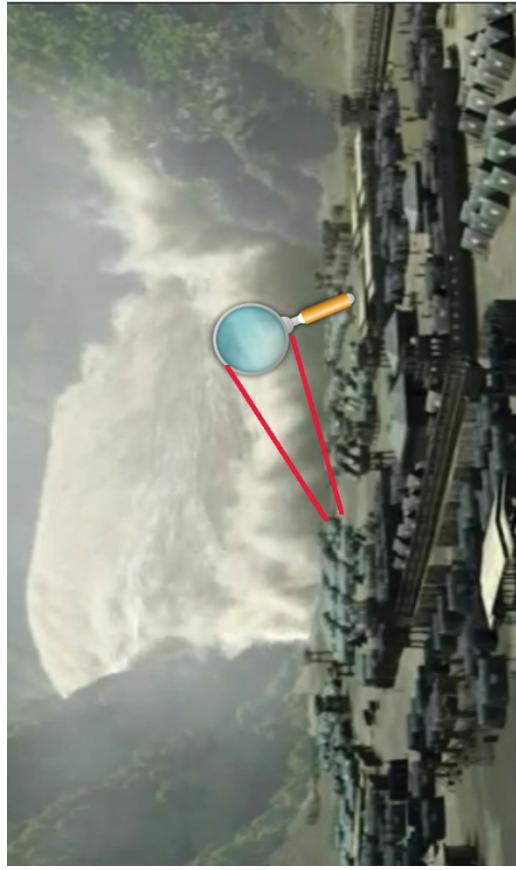


Large Simulations



Speed Up

- Large Models
 - Simulate at lower resolution
 - Use estimated data to do detailed simulation in key areas.
 - Run more smaller simulations on distributed machines
 - Only calculate 1 frame per sec





Idaho National Laboratory

Particle/Fluid Solvers

- Math started in the 50's and 60's (Los Alamos)
- Surface properties
- Volume interactions
 - Conservation of Mass
 - Conservation of momentum or energy
 - Conservation of volume
 - Connective acceleration
 - Viscosity
 - Boundary conditions
- Full solutions not possible, balance computer power and compromise
 - Methods(FLIP, SPH, Grid, MAC, PIC)

Expanding Possibilities

- Virtual Walk through using 3D model
 - Improve understanding of a system
 - Selectable components for information
- Interactive Risk Monitor
 - Select components in a virtual environment (no need to know the PRA model)
 - Set the date/time to remove component from service
- Sensor Alarms indicated in 3D model for easy understanding of where the problem is located

Questions

